1 / 1

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-030613
(43)Date of publication of application : 31.01.2003

(51)Int.Cl. G06K 19/073
G06K 17/00
G11C 16/02

(21)Application number : 2001-213036
(22)Date of filing : 13.07.2001

(71)Applicant : HITACHI LTD
(72)Inventor : TSUNODA MOTOYASU
MIZUSHIMA EIGA
KATAYAMA KUNIHIRO

(54) STORAGE DEVICE AND DATA PROCESSOR PROVIDED WITH THE STORAGE DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To improve the handleability of a card type storage device.
SOLUTION: The card type storage device 3610 is provided with a plurality of controller chips (3620 and 3630) and provided with a means supporting interface modes corresponding to the respective chips and switching and discriminating the mode by mode selection signals 3680.

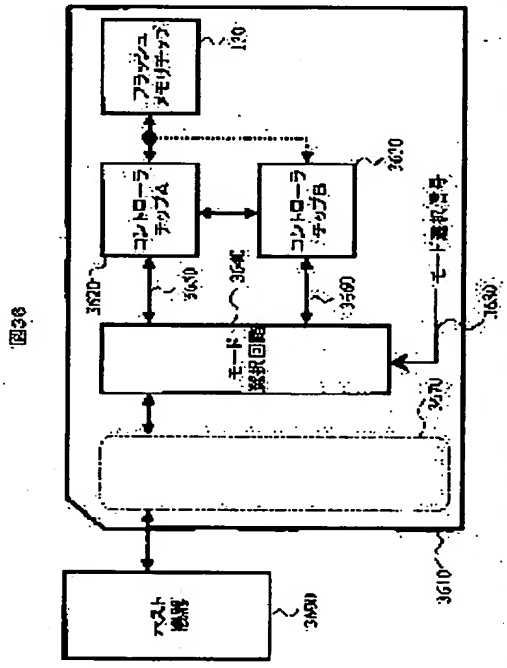


図36

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－30613
（P2003－30613A）
(43)公開日　平成15年１月31日(2003.1.31)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ	19/073	Ｇ０６Ｋ	17/00	Ｓ　５Ｂ０２５
	17/00		19/00	Ｐ　５Ｂ０３５
Ｇ１１Ｃ	16/02	Ｇ１１Ｃ	17/00	６０１Ｐ　５Ｂ０５８
				６０１Ｅ

審査請求　未請求　請求項の数７　ＯＬ　（全 32 頁）

(21)出願番号　特願2001－213036(P2001－213036)

(22)出願日　平成13年７月13日(2001.7.13)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　角田　元泰
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　水島　永雅
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　記憶装置及び記憶装置を備えたデータ処理装置

(57)【要約】
【課題】本発明は、カード型記憶装置の使い勝手を向上することを目的とする。
【解決手段】本発明は、カード型記憶装置３６１０において、複数のコントローラチップ（３６２０、３６３０）を備え、各々のチップに対応したインターフェースモードをサポートし、モードの切り替え及び判別をモード選択信号３６８０によって行う手段とを備える。

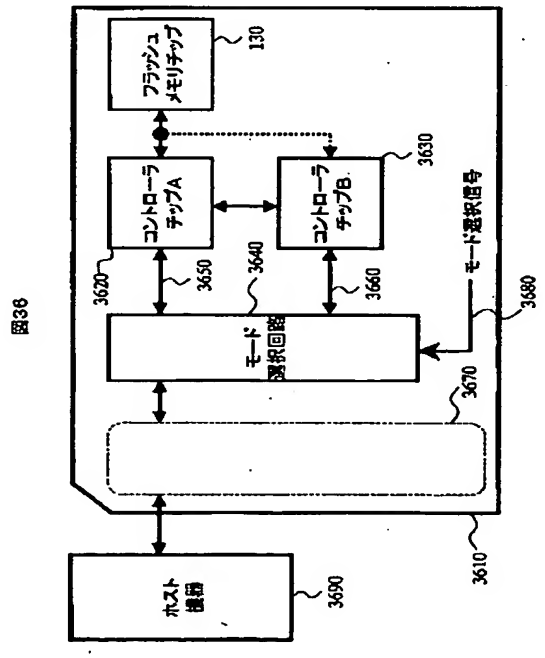


図38

【特許請求の範囲】

【請求項１】ホスト機器と接続される外部端子と、少なくとも２つのインターフェースモードを制御する制御手段と、前記少なくとも２つのインターフェースモードから１つのインターフェースモードを選択する選択手段と、前記選択手段による選択結果に基づき、選択された前記インターフェースモードで前記外部端子を制御する外部端子制御手段とを有することを特徴とする記憶装置。

【請求項２】前記制御手段は、前記少なくとも２つのインターフェースモードのうち、第１のインターフェースモードを制御するコントローラチップと、第２のインターフェースモードを制御するコントローラチップとを有し、前記外部端子制御手段は、前記選択されたインターフェースモードを制御するコントローラチップの外部入出力信号と前記外部端子とを接続する手段とを備えることを特徴とする請求項１記載の記憶装置。

【請求項３】記憶装置に記憶されたデータを用いてデータの処理を行うデータ処理装置において、前記記憶装置を制御する制御手段と、前記記憶装置が挿入されるソケットと、前記ソケット及び前記制御手段と接続される、インターフェースモードを検出する検出手段と、前記検出手段による検出結果がＩＣカードモードの場合に、前記ソケットと前記制御手段の信号線とを接続する手段とを有することを特徴とするデータ処理装置。

【請求項４】前記ソケットは、前記記憶装置が挿入されたことを検出する第１のスイッチと、前記第１のスイッチによって反応する第２のスイッチを有し、前記第２のスイッチによって前記記憶装置におけるインターフェースモードのサポート状態を検出するサポート検出手段と、前記サポート検出手段の検出結果に基づき、前記記憶装置のインターフェースモードを判定する手段とを有することを特徴とする請求項３記載のデータ処理装置。

【請求項５】ホスト機器が有するスイッチに応答する第３のスイッチを有し、前記第３のスイッチの状態によりインターフェースモードを選択する選択手段と、前記選択手段によって選択されたインターフェースモードで前記外部端子を制御する手段とを有することを特徴とする請求項１記載の記憶装置。

【請求項６】該記憶装置は、カード型記憶装置であって、カード同一辺上の両端に誤挿入防止のための第１の切り込み及び第２の切り込みを有し、前記第１の切り込みによって第１のインターフェースモードを一義的に決定するための手段と、前記第２の切り込みによって第２のインターフェースモードを一義的に決定するための手段とを有することを特徴とする請求項１記載の記憶装置。

【請求項７】カード型記憶装置に記憶されたデータを用いてデータの処理を行うデータ処理装置において、第４のスイッチと、前記第４のスイッチの状態に応じて、第１のインターフェースモードまたは第２のインターフェースモードを選択する選択手段と、前記選択手段によって選択されたインターフェースモードに基づきデータを処理する手段とを有することを特徴とするデータ処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、セキュリティ機能を有する記憶装置、その記憶装置が挿入可能なホスト機器、及びその記憶装置が挿入されたホスト機器に係り、特に、フラッシュメモリチップ及びコントローラを有するメモリカード、そのメモリカードが挿入可能な装置、並びにそのメモリカードが挿入された端末装置に関する。

【０００２】

【従来の技術】ＩＣカードは、プラスチックカード基板中にＩＣ（集積回路）チップを埋め込んだものであり、その表面にＩＣチップの外部端子を持つ。ＩＣチップの外部端子には電源端子、クロック端子、データ入出力端子などがある。ＩＣチップは、接続装置が外部端子から電源や駆動クロックを直接供給することによって動作する。ＩＣカードは、外部端子を通して端末機などの接続装置との間で電気信号を送受信することにより、接続装置と情報交換をおこなう。情報交換の結果として、ＩＣカードは計算結果や記憶情報の送出、記憶情報の変更をおこなう。ＩＣカードは、これらの動作仕様に基づいて、機密データ保護や個人認証などのセキュリティ処理を実行する機能を持つことができる。ＩＣカードは、クレジット決済やバンキングなど機密情報のセキュリティが必要とされるシステムにおいて、個人識別のためのユーザデバイスとして利用されている。

【０００３】

【発明が解決しようとする課題】セキュリティシステムにおいて利用されるＩＣカードは、秘密情報を用いて演算を行う際に、その秘密情報あるいはその秘密情報を推定できるような情報をＩＣカードの外部にもらさないように設計される必要がある。すなわち、耐タンパ性を持つことが必要とされる。このようなＩＣカードの外部にもらしてはならない秘密情報を解析する攻撃方法としては、タイミング解析、電力差分解析、故障利用解析などが知られている。

【０００４】タイミング解析は、暗号処理時間が秘密情報の内容に依存して異なる場合、その時間差を統計的に解析して秘密情報を推定する攻撃法である。暗号アルゴリズムを実装する際、処理時間の短縮やプログラムサイズの縮小を目的として、秘密情報の内容に依存して不要処理をスキップしたり分岐処理を行ったりするような最適化を適用することがある。このような最適化を適用すると、暗号処理時間が秘密情報の内容に依存して異なる。そのため処理時間を見ることで秘密情報の内容を推

定できる可能性がある。

【０００５】電力差分解析は、暗号処理の実行中にＩＣカードの電源端子から供給される電力を測定し、そこから消費電力の差分を解析することにより秘密情報を推定する攻撃法である。

【０００６】故障利用解析は、ＩＣカードの計算誤りを利用した攻撃法である。ＩＣカードに一過性の故障あるいは他の機能に影響を与えない範囲の限定的な障害を与え、ＩＣカードに攻撃者の望む異常な処理を行わせる。ＩＣカードに高電圧を加えたり、瞬間的にクロック周波数や駆動電圧を変動させることにより故意にエラーを発生させた場合、その結果得られる誤った計算結果と正しい計算結果から秘密情報が得られる可能性がある。

【０００７】ＩＣカードは、実用上、これらの攻撃法に対する対策手段を持たなければならない。

【０００８】本発明の目的は、セキュリティを向上した記憶装置を提供することである。

【０００９】また、ＩＣカードはクレジットカードサイズの形状のものが主流であるが、小型の携帯端末で用いる場合は大きく使い勝手が悪い。本発明の他の目的は、ＩＣカードの使い勝手を向上した記憶装置を提供することにある。

【００１０】

【課題を解決するための手段】上記課題を解決するため、本発明は、データを記憶するための記憶装置において、ホストと通信するための外部端子と、少なくとも２系統のホストインタフェースを制御する手段と、インタフェースを選択する手段と、該選択結果に基づき、選択されたインタフェースを該外部端子に接続する手段とを備える。

【００１１】上記、少なくとも２系統のホストインタフェースは、ホストインタフェースを制御する少なくとも２系統のコントローラチップにより制御され、該選択されたホストインタフェースを制御するコントローラチップの外部入出力信号と該外部端子を接続する手段とを備える。

【００１２】又は、本発明は、ＩＣカードに記憶されたデータを用いて処理するデータ処理装置において、ＩＣカードを制御する手段と、該記憶装置を挿入するためのソケットと、該ソケットと該制御手段との中間に配置され、インターフェースモードを検出する手段と、該検出結果がＩＣカードモードの場合において該ソケットと該制御手段の信号線を接続する手段とを備える。

【００１３】上記、該ソケットは、該記憶装置が挿入されたことを検出する第１のスイッチと、第１のスイッチによって反応する第２のスイッチを具備し、第２のスイッチによって該記憶装置におけるインターフェースモードのサポート状態を検出する手段と、該検出結果に基づき、ＩＣカードモードを判定する手段とを備える。

【００１４】また、該記憶装置は、該第２のスイッチによって反応し、インターフェースモードを選択する第３のスイッチを有し、該第３のスイッチの状態によりインタフェースを選択し、選択されたインタフェースを該外部端子に接続する手段とを備える。

【００１５】又は、本発明は、データを記憶するためのカード型記憶装置において、カード同一辺上の両端に誤挿入防止のための第１の切り込みと第２の切り込みを具備し、該第１の切り込みによって第１のインタフェースを一義的に決定するための手段と、該第２の切り込みによって第２のインタフェースを一義的に決定するための手段とを備える。また、該カード型記憶装置に記憶されたデータを用いて処理するデータ処理装置において、第４のスイッチを具備し、該記憶装置を挿入した場合において、該第４のスイッチにより、第１のインタフェースまたは第２のインタフェースを選択する手段と、該選択されたインタフェースに基づきデータを処理する手段とを備える。

【００１６】

【発明の実施の形態】図２２は、本発明を適用したＭｕｌｔｉＭｅｄｉａＣａｒｄ（ＭｕｌｔｉＭｅｄｉａＣａｒｄはＩｎｆｉｎｅｏｎＴｅｃｈｎｏｌｏｇｉｅｓＡＧの登録商標である。以下、「ＭＭＣ」と略記する。）の内部構成を簡単に表した図である。ＭＭＣ１１０は、ＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠するのが好ましい。ＭＭＣ１１０は、外部に接続したホスト機器２２０がＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠したメモリカードコマンドを発行することによって、機密データ保護や個人認証などに必要な暗号演算をおこなうセキュリティ処理機能を持つ。ホスト機器２２０は、例えば、携帯電話、携帯情報端末（ＰＤＡ）、パーソナルコンピュータ、音楽再生（及び録音）装置、カメラ、ビデオカメラ、自動預金預払器、街角端末、決済端末等が該当する。

【００１７】ＭＭＣ１１０は、ＭＭＣ外部端子１４０、コントローラチップ１２０、フラッシュメモリチップ１３０、ＩＣカードチップ１５０を持つ。フラッシュメモリチップ１３０は、不揮発性の半導体メモリを記憶媒体とするメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。ＭＭＣ外部端子１４０は７つの端子から構成され、外部のホスト機器２２０と情報交換するために、電源供給端子、クロック入力端子、コマンド入出力端子、データ入出力端子、グランド端子を含む。コントローラチップ１２０は、ＭＭＣ１１０内部の他の構成要素（ＭＭＣ外部端子１４０、フラッシュメモリチップ１３０、ＩＣカードチップ１５０）と接続されており、これらを制御するマイコンチップである。ＩＣカードチップ１５０は、ＩＣカードのプラスチック基板中に埋め込むためのマイコンチップであり、その外部端子、電気信号プロトコル、コマンドはＩＳＯ／ＩＥＣ７８１６規格に準拠している。ＩＣカードチップ

１５０の外部端子には、電源供給端子、クロック入力端子、リセット入力端子、Ｉ／Ｏ入出力端子、グランド端子がある。コントローラチップ１２０は、ＩＣカードチップ１５０の外部端子からＩＣカードチップ１５０にＩＣカードコマンドを発行することによって、外部のホスト機器２２０から要求されたセキュリティ処理に必要な演算をおこなう。

【００１８】図２６は、本発明のＩＣカードチップの内部構成を示す図である。ＩＣカードチップ１５０は、演算処理を行うためのＣＰＵ（マイコン）１５８と、データ（プログラムを含む。）を記憶するためのＲＯＭ（Read Only Memory）１５９とＲＡＭ（Random Access Memory）１６０とＥＥＰＲＯＭ（Electrically ErasableProgrammable ＲＯＭ）１６２と、暗号／復号に間する処理を行うための暗号コプロセッサ１６３と、外部とデータを送受信するためのシリアルインターフェース１６１とを備え、それらは、バス１６４によって接続される。そして、その暗号コプロセッサ１６３によって、ホスト機器２２０からのコマンドに応じて、ＩＣカードチップ１５０自らが、セキュリティ処理を実行することが可能である。尚、暗号コプロセッサ１６３（ハードウェア）の替わりに、プログラム（ソフトウェア）に従ってＣＰＵ１５８がセキュリティ処理を実行してもよい。

【００１９】一方、フラッシュメモリチップ１３０は、記憶素子を備えるが、マイコンは存在しない。セキュリティ処理は、例えば、ＩＣカードチップ１５０内の記憶領域にデータが書き込まれるとき、又は、ＩＣカードチップ１５０内の記憶領域からデータが読み出されるときに実行される。ＩＣカードチップ１５０のＥＥＰＲＯＭの記憶容量は、フラッシュメモリチップ１３０の記憶容量より小さい。但し、ＩＣカードチップ１５０のＥＥＰＲＯＭの記憶容量は、フラッシュメモリチップ１３０の記憶容量と同じでもよいし、大きくてもよい。

【００２０】ＩＣカードチップ１５０には、セキュリティ評価基準の国際標準であるＩＳＯ／ＩＥＣ１５４０８の評価・認証機関によって認証済みである製品を利用する。一般に、セキュリティ処理をおこなう機能を持つＩＣカードを実際の電子決済サービスなどで利用する場合、そのＩＣカードはＩＳＯ／ＩＥＣ１５４０８の評価・認証機関による評価と認定を受ける必要がある。ＭＭＣにセキュリティ処理をおこなう機能を追加することによってＭＭＣ１１０を実現し、それを実際の電子決済サービスなどで利用する場合、ＭＭＣ１１０も同様にＩＳＯ／ＩＥＣ１５４０８の評価・認証機関による評価と認定を受ける必要がある。本発明によれば、ＭＭＣ１１０は、評価・認証機関によって認証済みのＩＣカードチップ１５０を内蔵し、そのＩＣカードチップ１５０を利用してセキュリティ処理をおこなう構造を持つことにより、セキュリティ処理機能を得る。したがって、ＭＭＣ１１０はＩＳＯ／ＩＥＣ１５４０８に基づくセキュリティ評価基準を容易に満足することができ、ＭＭＣにセキュリティ処理機能を追加するための開発期間を短縮することができる。

【００２１】ＭＭＣ１１０は、ＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した外部インタフェースを持つのが好ましい。ＭＭＣ１１０は、一種類の外部インタフェースを通じて、標準メモリカードコマンド（フラッシュメモリチップ１３０へアクセスするためのコマンド）に加えて、セキュリティ処理を実行するコマンドを受け付ける必要がある。コントローラチップ１２０は、ＭＭＣ１１０が受信したコマンドが標準メモリカードコマンドであるか、セキュリティ処理を実行するコマンドであるかによって、アクセスすべきチップを選択し、コマンド処理を分配する機能を持つ。本発明によれば、標準メモリカードコマンドを受信したならば、フラッシュメモリチップ１３０を選択し、これにフラッシュメモリコマンドを発行してホストデータを読み書きできる。また、セキュリティ処理を実行するコマンドを受信したならば、ＩＣカードチップ１５０を選択し、これにＩＣカードコマンドを発行してセキュリティ処理を実行することができる。

【００２２】ＩＣカードチップ１５０の外部端子は、グランド端子を除いて、電源供給端子、クロック入力端子、リセット入力端子、Ｉ／Ｏ入出力端子がコントローラチップ１２０に接続されている。

【００２３】コントローラチップ１２０は、電源供給端子、クロック入力端子を通して、ＩＣカードチップ１５０への電源供給、クロック供給を制御する。本発明によれば、ホスト機器２２０からセキュリティ処理を要求されないときには、ＩＣカードチップ１５０への電源供給やクロック供給を停止させることができ、ＭＭＣ１１０の電力消費を削減することができる。電源供給されていないＩＣカードチップ１５０を、ＩＣカードコマンドを受信できる状態にするには、まず、ＩＣカードチップ１５０に電源供給を開始し、リセット処理を施すことが必要である。コントローラチップ１２０は、ＭＭＣ１１０がホスト機器２２０からセキュリティ処理を実行するコマンドを受信したのを契機に、電源供給端子を通してＩＣカードチップ１５０への電源供給を開始する機能を持つ。また、コントローラチップ１２０は、ＭＭＣ１１０がホスト機器２２０からセキュリティ処理を実行するコマンドを受信したのを契機に、リセット入力端子を通してＩＣカードチップ１５０のリセット処理をおこなう機能を持つ。本発明によれば、コントローラチップ１２０は、セキュリティ処理を実行するコマンドを受信するまでＩＣカードチップ１５０への電源供給を停止させておくことができる。したがって、ＭＭＣ１１０の電力消費を削減することができる。

【００２４】コントローラチップ１２０は、ＩＣカードチップ１５０のクロック入力端子を通してＩＣカードチ

ップ１５０に供給するクロック信号をＭＭＣ１１０内部で発生し、その周波数、供給開始タイミング、供給停止タイミングを制御する機能を持つ。本発明によれば、ＭＭＣ外部端子１４０のクロック入力端子のクロック信号と無関係にすることができるため、ホスト機器２２０によるタイミング解析、電力差分解析、故障利用解析と呼ばれる攻撃法に対してセキュリティが向上する。

【００２５】図２１は、フラッシュメモリチップ１３０の詳細な内部構成を表した図である。フラッシュメモリチップ１３０は、ホストデータ領域２１１５と管理領域２１１０とを含む。ホストデータ領域２１１５は、セクタ単位に論理アドレスがマッピングされている領域であり、ホスト機器２２０が論理アドレスを指定してデータを読み書きできる領域である。ホストデータ領域２１１５は、ユーザファイル領域２１３０とセキュリティ処理アプリケーション領域２１２０とを含む。ユーザファイル領域２１３０は、ユーザが自由にファイルデータを読み書きできる領域である。セキュリティ処理アプリケーション領域２１２０は、ホスト機器２２０がセキュリティ処理アプリケーションに必要なデータを格納する領域であり、ユーザが不正にアクセスしないように、ホスト機器２２０のセキュリティ処理アプリケーションが論理的にユーザアクセス制限をかける。ここに格納するデータとしては、ホスト機器２２０のアプリケーションプログラム、そのアプリケーション専用のデータ、セキュリティ処理に使用される証明書など（例えば、電子決済アプリケーションプログラム、電子決済ログ情報、電子決済サービス証明書など）が可能である。本発明によれば、ＭＭＣ１１０が、ホスト機器２２０がセキュリティ処理をおこなう上で使用するデータをホスト機器２２０の代わりに格納するため、ホスト機器２２０にとって利便性が向上する。

【００２６】一方、管理領域２１１０は、コントローラチップ１２０がＩＣカードチップ１５０を管理するための情報を格納する領域である。管理領域２１１０は、ＩＣカード制御パラメータ領域２１１１、ＩＣカード環境設定情報領域２１１２、ＣＬＫ２設定情報領域２１１３、セキュリティ処理バッファ領域２１１４、セキュリティ処理ステータス領域２１１６とを含む。２１１１～２１１６の領域の詳細な使用法については後述する。

【００２７】コントローラチップ１２０は、フラッシュメモリチップ１３０の管理領域２１１０のセキュリティ処理バッファ領域２１１４を、ＩＣカードチップ１５０でセキュリティ処理を実行する際のメインメモリまたはバッファメモリとして利用する。ホスト機器２２０がセキュリティ処理を実行するコマンドによりＭＭＣ１１０にアクセスした際に、ＭＭＣ１１０がホスト機器２２０からＩＣカードチップ１５０に一度に送信できないほどの大きなサイズのセキュリティ関連データを受信したならば、コントローラチップ１２０はフラッシュメモリチップ１３０へのアクセスを選択し、そのデータを十分な容量を持つセキュリティ処理バッファ領域２１１４に一時的に格納する。ＩＣカードチップ１５０に一度に送信できないほどのサイズは、ＩＣカードコマンドの許容データサイズ（例えば、２５５バイト又は２５６バイト）を超えるサイズである。そして、コントローラチップ１２０はそれをＩＣカードチップ１５０に送信できるサイズのデータに分割し、分割データをフラッシュメモリチップ１３０から読み出し、段階的にＩＣカードチップ１５０に送信する。つまり、分割されたデータの読み出し、書き込みを繰り返す。本発明によれば、ホスト機器２２０にとって、大きなサイズのセキュリティ関連データを扱うことができるので、セキュリティ処理の利便性が向上する。

【００２８】セキュリティ処理バッファ領域２１１４を含む管理領域２１１０は、ホスト機器２２０が不正にアクセスしてセキュリティ処理を解析することができないように、コントローラチップ１２０により物理的にホストアクセス制限がかけられている。つまり、管理領域２１１０はホスト機器２２０が直接データを読み書きできない。本発明によれば、ホスト機器２２０がセキュリティ処理バッファ領域２１１４の内容を自由に読み出したり改ざんすることができないため、セキュリティ処理の信頼性や安全性が向上する。

【００２９】図２３は、ＭＭＣ１１０を利用したセキュリティ処理の一例として、コンテンツ配信のセキュリティ処理を表したものである。コンテンツプロバイダ２３１０は、ＭＭＣ１１０を所有するユーザにコンテンツ２３１４を販売する業者である。ホスト機器２２０は、この例では、コンテンツプロバイダ２３１０とネットワークなどを介して接続することができる端末機である。ユーザはＭＭＣ１１０をホスト機器２２０に接続してコンテンツ２３１４を購入する。以下、その手順を説明する。

【００３０】まず、ホスト機器２２０はＭＭＣ１１０に、フラッシュメモリチップ１３０に格納されたユーザ証明書２３２１を読み出すコマンドを発行する。ＭＭＣ１１０のコントローラチップ１２０は、フラッシュメモリチップ１３０のセキュリティ処理アプリケーション領域２１２０に格納されたユーザ証明書２３２１を読み出し、それをホスト機器２２０に送信する。そして、ホスト機器２２０はそれをコンテンツプロバイダ２３１０に送信する。コンテンツプロバイダ２３１０はユーザ証明書２３２１につけられたデジタル署名を検証する（２３１１）。検証が成功したならば、乱数発生器によりセッション鍵を生成し（２３１２）、それをユーザ証明書２３２１から抽出したユーザ公開鍵によって暗号化する（２３１３）。さらに、コンテンツ２３１４をそのセッション鍵によって暗号化する（２３１５）。

【００３１】コンテンツプロバイダ２３１０はステップ

２３１３の結果をホスト機器２２０に送信する。ホスト機器２２０は、ステップ２３１３の結果をユーザ秘密鍵２３２２によって復号するセキュリティ処理を要求するコマンドを、ＭＭＣ１１０に発行する。コントローラチップ１２０は、ステップ２３１３の結果をユーザ秘密鍵２３２２によって復号するＩＣカードコマンドを、ＩＣカードチップ１５０に発行する。ＩＣカードチップ１５０は、ユーザ秘密鍵２３２２によってステップ２３１３の結果を復号して、セッション鍵を取得する（２３２３）。ホスト機器２２０は、この復号処理が成功したかを示す情報を出力させるコマンドをＭＭＣ１１０に発行する。コントローラチップ１２０は、ＩＣカードチップ１５０の出力する復号結果（復号処理が成功したかを示すＩＣカードレスポンス）をもとにしてホスト機器２２０の求める情報を構築する。そして、ＭＭＣ１１０はその情報をホスト機器２２０に送信する。

【００３２】次に、コンテンツプロバイダ２３１０は、ステップ２３１５の結果を、ホスト機器２２０に送信する。ホスト機器２２０は、ステップ２３１３の結果をセッション鍵（ステップ２３２３によって取得した鍵）によって復号するセキュリティ処理を要求するコマンドを、ＭＭＣ１１０に発行する。コントローラチップ１２０は、ステップ２３１５の結果をセッション鍵によって復号するＩＣカードコマンドを、ＩＣカードチップ１５０に発行する。ＩＣカードチップ１５０は、セッション鍵によってステップ２３１５の結果を復号して、コンテンツ２３１４を復元する（２３２４）。コントローラチップ１２０は、このコンテンツ２３１４をＩＣカードチップ１５０から受信し、フラッシュメモリチップ１３０に書きこむ。ホスト機器２２０は、この復号処理が成功したかを示す情報を出力させるコマンドをＭＭＣ１１０に発行する。コントローラチップ１２０は、ＩＣカードチップ１５０の出力する復号結果（復号処理が成功したかを示すＩＣカードレスポンス）をもとにしてホスト機器２２０の求める情報を構築する。そして、ＭＭＣ１１０はその情報をホスト機器２２０に送信する。ホスト機器２２０が、コンテンツを無事に受信したことをコンテンツプロバイダ２３１０に伝えると、コンテンツプロバイダ２３１０はユーザ証明書に記載されたユーザにコンテンツ料金を課金する。

【００３３】ユーザは、ホスト機器２２０でＭＭＣ１１０内のフラッシュメモリチップ１３０に格納されたコンテンツ２３１４を読み出して利用することができる。また、フラッシュメモリチップ１３０の記憶媒体に大容量のフラッシュメモリを使用すれば、多くのコンテンツを購入できる。本発明によれば、コンテンツ配信におけるセキュリティ処理とコンテンツ蓄積の両方をＭＭＣ１１０によって容易に実現できる。コンテンツ料金の決済を、ＩＣカードチップ１５０を利用して行ってもよい。

【００３４】図２４と図２５は、それぞれ、本発明をＳＤカード（幅２４ミリメートル、長さ３２ミリメートル、厚さ２。１ミリメートルで、９つの外部端子をもち、フラッシュメモリを搭載した小型メモリカードである。）とメモリースティック（メモリースティックはソニー株式会社の登録商標である。）に適用したときの簡単な内部構成図を表したものである。本発明を適用したＳＤカード２４１０は、ＳＤカードコントローラチップ２４２０、フラッシュメモリチップ２４３０、ＳＤカード外部端子２４４０、ＩＣカードチップ１５０とを含む。本発明を適用したメモリースティック２５１０は、メモリースティックコントローラチップ２５２０、フラッシュメモリチップ２５３０、メモリースティック外部端子２５４０、ＩＣカードチップ１５０とを含む。フラッシュメモリチップ２４３０と２５３０は、不揮発性の半導体メモリを記憶媒体とするメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。ＳＤカードコントローラチップ２４２０とメモリースティックコントローラチップ２５２０はそれぞれＳＤカードとメモリースティック内の他の構成要素を制御するマイコンチップである。

【００３５】ＳＤカード外部端子２４４０は９つの端子からなり、それらの位置は、端からＤａｔａ２端子２４４１、Ｄａｔａ３端子２４４２、Ｃｏｍ端子２４４３、Ｖｓｓ端子２４４４、Ｖｄｄ端子２４４５、Ｃｌｏｃｋ端子２４４６、Ｖｓｓ端子２４４７、Ｄａｔａ０端子２４４８、Ｄａｔａ１端子２４４９の順で並んでいる。Ｖｄｄ端子２４４５は電源供給端子、Ｖｓｓ端子２４４４と２４４７はグランド端子、Ｄａｔａ０端子２４４８とＤａｔａ１端子２４４９とＤａｔａ２端子２４４１とＤａｔａ３端子２４４２はデータ入出力端子、Ｃｏｍ端子２４４３はコマンド入出力端子、Ｃｌｏｃｋ端子２４４６はクロック入力端子である。ＳＤカード２４１０は、外部に接続するＳＤカードホスト機器２４６０とのインタフェース仕様にＭＭＣ１１０と違いがあるものの、ＭＭＣ外部端子１４０と非常に類似した外部端子を持ち、ＭＭＣ１１０と同様に外部からコマンドを発行することにより動作する特徴を持つため、本発明を適用することができる。

【００３６】一方、メモリースティック外部端子２５４０は１０個の端子からなり、それらの位置は、端からＧｎｄ端子２５４１、ＢＳ端子２５４２、Ｖｃｃ端子２５４３、予約端子Ｒｓｖを１つ飛ばしてＤＩＯ端子２５４４、ＩＮＳ端子２５４５、予約端子Ｒｓｖを１つ飛ばしてＳＣＫ端子２５４６、Ｖｃｃ端子２５４７、Ｇｎｄ端子２５４８の順で並んでいる。Ｖｃｃ端子２５４３と２５４７は電源供給端子、Ｇｎｄ端子２５４１と２５４８はグランド端子、ＤＩＯ端子２５４４はコマンドおよびデータ入出力端子、ＳＣＫ端子２５４６はクロック入力端子である。メモリースティック２５１０は、外部に接続するメモリースティックホスト機器２５６０とのイン

タフェース仕様にＭＭＣ１１０と違いがあるものの、ＭＭＣ１１０と同様に外部からコマンドを発行することにより動作する特徴を持つため、本発明を適用することができる。

【００３７】図１は、本発明を適用したＭＭＣの詳細な内部構成図を表したものである。また、図２は、図１のＭＭＣ１１０と接続したホスト機器２２０の構成とその接続状態を表したものである。ホスト機器２２０は、ＶＣＣ１電源２２１、ＣＬＫ１発振器２２２、ホストインタフェース２２３を持つ。

【００３８】ＭＭＣ１１０は、外部のホスト機器２２０と情報交換するためのＭＭＣ外部端子１４０を持つ。ＭＭＣ外部端子１４０は、ＣＳ端子１４１、ＣＭＤ端子１４２、ＧＮＤ１端子１４３および１４６、ＶＣＣ１端子１４４、ＣＬＫ１端子１４５、ＤＡＴ端子１４７の７つの端子とを含む。ＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様は、ＭＭＣの動作モードとしてＭＭＣモードとＳＰＩモードという２種類を規定しており、動作モードによってＭＭＣ外部端子１４０の使用法は異なる。本実施例ではＭＭＣモードでの動作の場合について詳細に説明する。

【００３９】ＶＣＣ１端子１４４は、ＶＣＣ１電源２２１と接続されており、ホスト機器２２０がＭＭＣ１１０に電力を供給するための電源端子である。ＧＮＤ１端子１４３および１４６は、ＶＣＣ１電源２２１と接続されており、ＭＭＣ１１０の電気的なグランド端子である。ＧＮＤ１端子１４３とＧＮＤ１端子１４６は、ＭＭＣ１１０内部で電気的に短絡されている。ＣＳ端子１４１は、ホストインタフェース２２３に接続されており、ＳＰＩモードの動作において使用される入力端子である。ホスト機器２２０が、ＭＭＣ１１０にＳＰＩモードでアクセスするときには、ＣＳ端子１４１にＬレベルを入力する。ＭＭＣモードの動作では、ＣＳ端子１４１を使用する必要はない。ＣＭＤ端子１４２は、ホストインタフェース２２３に接続されており、ホスト機器２２０が、メモリカードインタフェース仕様に準拠したメモリカードコマンドをＭＭＣ１１０に送信したり、同仕様に準拠したメモリカードレスポンスをＭＭＣ１１０から受信するために使用する入出力端子である。

【００４０】ＤＡＴ端子１４７は、ホストインタフェース２２３に接続されており、ホスト機器２２０が、メモリカードインタフェース仕様に準拠した形式の入力データをＭＭＣ１１０に送信したり、同仕様に準拠した形式の出力データをＭＭＣ１１０から受信するために使用する入出力端子である。ＣＬＫ１端子１４５は、ＣＬＫ１発振器２２２に接続されており、ＣＬＫ１発振器２２２が生成するクロック信号が入力される端子である。ホスト機器２２０が、ＣＭＤ端子１４２を通してメモリカードコマンド、メモリカードレスポンスを送受信したり、ＤＡＴ端子１４７を通してホストデータを送受信するときに、ＣＬＫ１端子１４５にクロック信号が入力される。ホストインタフェース２２３には、ＣＬＫ１発振器２２２からクロック信号が供給されており、メモリカードコマンド、メモリカードレスポンス、ホストデータは、ＣＬＫ１発振器２２２が生成するクロック信号にビット単位で同期して、ホスト機器２２０とＭＭＣ１１０との間を転送される。

【００４１】ＭＭＣ１１０は、コントローラチップ１２０を持つ。コントローラチップ１２０は、ＣＰＵ１２１、フラッシュメモリＩ／Ｆ制御回路１２２、ＭＭＣＩ／Ｆ制御回路１２３、ＣＬＫ０発振器１２４、ＶＣＣ２生成器１２５、ＶＣＣ２制御回路１２６、ＣＬＫ２制御回路１２７、ＩＣカードＩ／Ｆ制御回路１２８とを含む。これらの構成要素１２１～１２８は、ホスト機器２２０からＶＣＣ１端子１４４やＧＮＤ１端子１４３、１４６を通して供給された電力により動作する。ＭＭＣＩ／Ｆ制御回路１２３は、ＣＳ端子１４１、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、ＤＡＴ端子１４７と接続されており、ＭＭＣ１１０がそれらの端子を通してホスト機器２２０と情報交換するためのインタフェースを制御する論理回路である。ＣＰＵ１２１は、ＭＭＣＩ／Ｆ制御回路１２３と接続されており、ＭＭＣＩ／Ｆ制御回路１２３を制御する。

【００４２】ＭＭＣＩ／Ｆ制御回路１２３がＣＭＤ端子１４２を通してホスト機器２２０からメモリカードコマンドを受信すると、ＭＭＣＩ／Ｆ制御回路１２３はそのコマンドの受信が成功したかどうかの結果をホスト機器２２０に伝えるためＣＭＤ端子１４２を通してホスト機器２２０にレスポンスを送信する。ＣＰＵ１２１は、受信したメモリカードコマンドを解釈し、コマンド内容に応じた処理を実行する。また、そのコマンド内容に応じてホスト機器２２０とＤＡＴ端子１４７を通してデータの送受信をおこなう必要がある場合、ＣＰＵ１２１は、ＭＭＣＩ／Ｆ制御回路１２３へのデータの送出、ＭＭＣＩ／Ｆ制御回路１２３からのデータの取得をおこなう。さらに、ＣＰＵ１２１は、ＭＭＣＩ／Ｆ制御回路１２３とホスト機器２２０との間のデータ転送手続きも制御する。例えば、ホスト機器２２０から受信したデータの処理中に、ホスト機器２２０がＭＭＣ１１０への電源供給を停止することがないように、ＣＰＵ１２１はＤＡＴ端子１４７にＬレベルを出力させ、ＭＭＣ１１０がビジー状態であることをホスト機器２２０に伝える。ＣＬＫ０発振器１２４は、ＣＰＵ１２１と接続され、ＣＰＵ１２１を動作させる駆動クロックを供給する。

【００４３】ＭＭＣ１１０は、フラッシュメモリチップ１３０を持つ。フラッシュメモリチップ１３０は、不揮発性の半導体メモリを記憶媒体とするメモリチップである。フラッシュメモリチップ１３０は、ホスト機器２２０からＶＣＣ１端子１４４やＧＮＤ１端子１４３、１４６を通して供給された電力により動作する。フラッシュメモリチップ１３０は、外部からのフラッシュメモリコ

マンドに従って、入力されたデータを不揮発性の半導体メモリに格納するライト機能、また同メモリに格納されたデータを外部に出力するリード機能を持つ。フラッシュメモリＩ／Ｆ制御回路１２２は、フラッシュメモリチップ１３０にフラッシュメモリコマンドを発行したり、そのコマンドで入出力するデータを転送するための論理回路である。ＣＰＵ１２１は、フラッシュメモリＩ／Ｆ制御回路１２２を制御し、フラッシュメモリチップ１３０にデータのライト機能やリード機能を実行させる。ホスト機器２２０から受信したデータをフラッシュメモリチップ１３０にライトしたり、フラッシュメモリチップ１３０に格納されたデータをホスト機器２２０に送信する必要があるとき、ＣＰＵ１２１は、フラッシュメモリＩ／Ｆ制御回路１２２とＭＭＣＩ／Ｆ制御回路１２３の間のデータ転送を制御する。

【００４４】ＭＭＣ１１０は、ＩＣカードチップ１５０を持つ。ＩＣカードチップ１５０は、ＩＣカードの基板中に埋め込むことを目的として設計されたＩＣチップであり、ＩＣカードの外部端子規格に準拠した８つの外部端子を持つ。このうち６つの端子は、ＩＣカードの外部端子規格により使用法が割り付けられており、残りの２つは将来のための予備端子である。その６つの端子は、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、ＧＮＤ２端子１５５、ＶＰＰ端子１５６、Ｉ／Ｏ端子１５７である。

【００４５】ＩＣカードチップ１５０のグランド端子は、ＭＭＣ外部端子１４０のＧＲＮ１（グランド端子）１４６に接続される。ＩＣカードチップ１５０のＶＣＣ２端子（電源入力端子）１５１は、コントローラチップ１２０のＶＣＣ２制御回路１２６に接続される。ＩＣカードチップ１５０のＲＳＴ端子（リセット入力端子）１５２とＩ／Ｏ端子（データ入出力端子）１５７は、コントローラチップ１２０のＩＣカードＩ／Ｆ制御回路１２８に接続される。ＩＣカードチップ１５０のＣＬＫ２端子（クロック入力端子）１５３は、コントローラチップ１２０のＣＬＫ２制御回路１２７に接続される。

【００４６】フラッシュメモリチップ１３０のＶＣＣ端子（電源入力端子）は、ＭＭＣ外部端子１４０のＶＣＣ１１４４に接続される。フラッシュメモリチップ１３０のＶＳＳ端子（グランド端子）は、ＭＭＣ外部端子１４０のＧＲＤ１１４６に接続される。フラッシュメモリチップ１３０のＩ／Ｏ端子（データ入出力端子）とレディ／ビジー端子とチップイネーブル端子とアウトプットイネーブル端子とライトイネーブル端子とクロック端子とリセット端子とは、コントローラチップ１２０のフラッシュメモリＩＦ制御回路１２２に接続される。

【００４７】ＶＣＣ２端子１５１は、ＩＣカードチップ１５０に電力を供給するための電源端子である。ＶＣＣ２制御回路１２６は、ＭＯＳ－ＦＥＴ素子を用いたスイッチ回路によりＶＣＣ２端子１５１への電力の供給開始と供給停止を制御する回路である。ＶＣＣ２生成器１２５はＶＣＣ２端子１５１に供給する電圧を発生し、それをＶＣＣ２制御回路１２６に供給する。ＩＣカードの電気信号規格はＩＣカードの動作クラスとしてクラスＡとクラスＢを規定している。ＶＣＣ２端子１５１に供給する標準電圧は、クラスＡでは５Ｖ、クラスＢでは３Ｖである。本発明はＩＣカードチップ１５０の動作クラスによらず適用できるが、本実施例ではＩＣカードチップ１５０がクラスＢで動作する場合について詳細に説明する。ＶＰＰ端子１５６は、ＩＣカードチップ１５０がクラスＡで動作する時に、内部の不揮発性メモリにデータを書き込んだり消去したりするために使用される可変電圧を供給する端子であり、クラスＢで動作する時には使用しない。ＧＮＤ２端子１５５は、ＩＣカードチップ１５０の電気的なグランド端子であり、ＧＮＤ１端子１４３、１４６と短絡されている。ＶＣＣ２制御回路１２６はＣＰＵ１２１と接続され、ＣＰＵ１２１はＶＣＣ２端子１５１への電力供給の開始と停止を制御することができる。ＩＣカードチップ１５０を使用しないときは、ＣＰＵ１２１はＶＣＣ２端子１５１への電力供給を停止することができる。ＭＭＣ１１０は、ＩＣカードチップ１５０への電力供給を停止することにより、それが消費する電力を節約することができる。ただし、電力供給を停止すると、ＩＣカードチップ１５０の内部状態は、ＩＣカードチップ１５０内部の不揮発性メモリに記憶されたデータを除いて維持されない。

【００４８】ＣＬＫ２端子１５３は、ＩＣカードチップ１５０にクロック信号を入力する端子である。ＣＬＫ２制御回路１２７は、ＣＬＫ２端子１５３にクロックを供給する回路である。ＣＬＫ２制御回路１２７は、ＣＬＫ０発振器１２４から供給されたクロック信号をもとにしてＣＬＫ２端子１５３に供給するクロック信号を生成する。ＣＬＫ２制御回路１２７はＣＰＵ１２１と接続されており、ＣＬＫ２端子１５３へのクロックの供給開始と供給停止をＣＰＵ１２１から制御することができる。ＩＣカードチップ１５０は、自身内部に駆動クロック発振器をもたない。そのため、ＣＬＫ２端子１５３から駆動クロックを供給することによって動作する。ＣＬＫ２制御回路１２７が、ＣＬＫ２端子１５３へのクロック供給を停止すると、ＩＣカードチップ１５０の動作は停止するため、ＩＣカードチップ１５０の消費電力を低下させることができる。この時、ＶＣＣ２端子１５１への電力供給が保たれていれば、ＩＣカードチップ１５０の内部状態は維持される。ここで、ＣＬＫ２端子１５３に供給するクロック信号の周波数をＦ２、ＣＬＫ０発振器１２４から供給されたクロック信号の周波数をＦ０、ＰとＱを正の整数とすると、ＣＬＫ２制御回路１２７は、Ｆ２＝（Ｐ／Ｑ）＊Ｆ０の関係になるようなクロック信号を作成して、これをＣＬＫ２端子１５３に供給する。ＰとＱの値はＣＰＵ１２１により設定できるようになってい

る。Ｐを大きく設定してＦ２を大きくすると、ＩＣカードチップ１５０の内部処理をより高速に駆動できる。Ｑを大きく設定してＦ２を小さくすると、ＩＣカードチップ１５０の内部処理はより低速に駆動され、ＩＣカードチップ１５０の消費電力を低下させることができる。ＩＣカードチップ１５０の駆動クロック周波数は、ＩＣカードチップ１５０が正しく動作できるような許容周波数範囲内に設定される必要がある。そのため、ＣＬＫ２制御回路１２７は、Ｆ２の値がその許容周波数範囲を外れるようなＰとＱの値を設定させない特徴を持つ。

【００４９】Ｉ／Ｏ端子１５７は、ＩＣカードチップ１５０にＩＣカードコマンドを入力したり、ＩＣカードチップ１５０がＩＣカードレスポンスを出力するときに使用する入出力端子である。ＩＣカードＩ／Ｆ制御回路１２８は、Ｉ／Ｏ端子１５７と接続されており、Ｉ／Ｏ端子１５７を通してＩＣカードコマンドの信号送信やＩＣカードレスポンスの信号受信をおこなう回路である。ＩＣカードＩ／Ｆ制御回路１２８はＣＰＵ１２１に接続されており、ＣＰＵ１２１は、ＩＣカードＩ／Ｆ制御回路１２８によるＩＣカードコマンドやＩＣカードレスポンスの送受信の手続きを制御したり、送信すべきＩＣカードコマンドデータをＩＣカードＩ／Ｆ制御回路１２８に設定したり、受信したＩＣカードレスポンスをＩＣカードＩ／Ｆ制御回路１２８から取得する。ＩＣカードＩ／Ｆ制御回路１２８にはＣＬＫ２制御回路１２７からクロックが供給されており、ＩＣカードコマンドやＩＣカードレスポンスは、ＣＬＫ２端子１５３に供給するクロック信号にビット単位で同期して、Ｉ／Ｏ端子１５７を通して送受信される。また、ＲＳＴ端子１５２は、ＩＣカードチップ１５０をリセットするときにリセット信号を入力する端子である。ＩＣカードＩ／Ｆ制御回路１２８は、ＲＳＴ端子１５２と接続されており、ＣＰＵ１２１の指示によりＩＣカードチップ１５０にリセット信号を送ることができる。

【００５０】ＩＣカードチップ１５０は、ＩＣカードの電気信号規格やコマンド規格に基づいて情報交換をおこなう。ＩＣカードチップ１５０へのアクセスパターンは４種類であり、図３～図６を用いて各パターンを説明する。図３は、ＣＰＵ１２１の指示によりＩＣカードチップ１５０が非活性状態（電源が遮断されている状態）から起動して内部状態を初期化するプロセス（以下、コールドリセットと呼ぶ）において、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図４は、ＣＰＵ１２１の指示によりＩＣカードチップ１５０が活性状態（電源が供給されている状態）で内部状態を初期化するプロセス（以下、ウォームリセットと呼ぶ）において、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図５は、ＣＰＵ１２１の指示によりＩＣカードチップ１５０にＩＣカードコマンドを送信しＩＣカードチップ１５０からＩＣカードレスポンスを受信するプロセスにおいて、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図６は、ＣＰＵ１２１の指示によりＩＣカードチップ１５０を非活性状態にするプロセスにおいて、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図３～図６において、時間の方向は左から右にとっており、上の行から下の行に向かってＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、Ｉ／Ｏ端子１５７で観測される信号を表す。また、破線はそれぞれの信号の基準（Ｌレベル）を表す。

【００５１】図３を参照して、ＩＣカードチップ１５０のコールドリセット操作を説明する。まず、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＬレベルにする（３０１）。次に、ＶＣＣ２制御回路１２６はＶＣＣ２端子への電源供給を開始する（３０２）。次に、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を開始する（３０３）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７を状態Ｚ（プルアップされた状態）にする（３０４）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＨレベルにする（３０５）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７から出力されるリセット応答の受信を開始する（３０６）。リセット応答の受信が終了したら、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を停止する（３０７）。これで、コールドリセットの操作が完了する。なお、ステップ３０７は消費電力を低下させるための工夫であり、省略してもよい。

【００５２】図４を参照して、ＩＣカードチップ１５０のウォームリセット操作を説明する。まず、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を開始する（４０１）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＬレベルにする（４０２）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７を状態Ｚにする（４０３）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＨレベルにする（４０４）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７から出力されるリセット応答の受信を開始する（４０５）。リセット応答の受信が終了したら、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を停止する（４０６）。これで、ウォームリセットの操作が完了する。なお、ステップ４０６は消費電力を低下させるための工夫であり、省略してもよい。

【００５３】図５を参照して、ＩＣカードチップ１５０にＩＣカードコマンドを送信しＩＣカードチップ１５０からＩＣカードレスポンスを受信する操作を説明する。まず、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を開始する（５０１）。なお、ク

ロックがすでに供給されている場合、ステップ５０１は不要である。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７にコマンドデータの送信を開始する（５０２）。コマンドデータの送信が終了したら、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７を状態Ｚにする（５０３）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７から出力されるレスポンスデータの受信を開始する（５０４）。レスポンスデータの受信が終了したら、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３へのクロック信号の供給を停止する（５０５）。これで、ＩＣカードコマンド送信とＩＣカードレスポンス受信の操作が完了する。なお、ステップ５０５は、消費電力を低下させるための工夫であり、省略してもよい。

【００５４】図６を参照して、ＩＣカードチップ１５０を非活性化する操作を説明する。まず、ＣＬＫ２制御回路１２７はＣＬＫ２端子１５３をＬレベルにする（６０１）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＲＳＴ端子１５２をＬレベルにする（６０２）。次に、ＩＣカードＩ／Ｆ制御回路１２８はＩ／Ｏ端子１５７をＬレベルにする（６０３）。最後に、ＶＣＣ２制御回路１２６はＶＣＣ２端子への電源供給を停止する（６０４）。これで、非活性化の操作が完了する。

【００５５】ＩＣカードチップ１５０は、機密データ保護や個人認証などに必要な暗号演算をおこなうセキュリティ処理機能を持つ。ＩＣカードチップ１５０は、ＣＰＵ１２１との間でＩＣカードコマンドやＩＣカードレスポンスの送受信することにより情報交換をおこない、その結果として、計算の結果や記憶されている情報の送出、記憶されている情報の変更などをおこなう。ＣＰＵ１２１は、ＩＣカードチップ１５０を利用してセキュリティ処理を実行することができる。ＭＭＣ１１０がホスト機器２２０から特定のメモリカードコマンドを受信すると、ＣＰＵ１２１はそれを契機として、ＶＣＣ２制御回路１２６を通してＩＣカードチップ１５０への電源供給を制御したり、またはＣＬＫ２制御回路１２７を通してＩＣカードチップ１５０へのクロック供給を制御したり、またはＩＣカードＩ／Ｆ制御回路１２８を通してＩＣカードチップ１５０にＩＣカードコマンドを送信する。これにより、ＣＰＵ１２１は、ＩＣカードチップ１５０を利用して、ホスト機器２２０が要求するセキュリティ処理を実行する。ＣＰＵ１２１は、特定のメモリカードコマンドの受信を契機に、ＩＣカードチップ１５０に対する電源供給制御、クロック供給制御、ＩＣカードコマンド送信、ＩＣカードレスポンス受信を複数組み合わせて操作することによって、セキュリティ処理を実行してもよい。また、ＣＰＵ１２１は、ホスト機器２２０がＭＭＣ１１０へ電源供給を開始したのを契機として、セキュリティ処理を実行してもよい。セキュリティ処理の結果は、ＩＣカードチップ１５０が出力するＩＣカードレスポンスをベースにして構成され、ＭＭＣ１１０内に保持される。ＭＭＣ１１０がホスト機器２２０から特定のメモリカードコマンドを受信すると、ＣＰＵ１２１はそれを契機として、セキュリティ処理の結果をホスト機器２２０に送信する。

【００５６】図７は、ホスト機器２２０がＭＭＣ１１０にアクセスするときのフローチャートを表したものである。まず、ホスト機器２２０はＭＭＣ１１０を活性化するためにＶＣＣ１端子１４４に電源供給を開始する（７０１）。これを契機として、ＭＭＣ１１０は、第１次ＩＣカード初期化処理を実行する（７０２）。第１次ＩＣカード初期化処理の詳細は後述する。次に、ホスト機器２２０はＭＭＣ１１０を初期化するためにＣＭＤ端子１４２を通してＭＭＣ１１０の初期化コマンドを送信する（７０３）。この初期化コマンドはＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠したものであり、複数種類ある。ホスト機器２２０は、ＭＭＣ１１０を初期化するために、複数の初期化コマンドを送信する場合がある。ＭＭＣ１１０が初期化コマンドを受信すると、ＭＭＣ１１０はそれを処理する（７０４）。これを契機として、ＭＭＣ１１０は、第２次ＩＣカード初期化処理を実行する（７０５）。第２次ＩＣカード初期化処理の詳細は後述する。ホスト機器２２０は、ＭＭＣ１１０の初期化コマンドに対するメモリカードレスポンスを、ＣＭＤ端子１４２を通して受信し、そのメモリカードレスポンスの内容からＭＭＣ１１０の初期化が完了したかを判定する。未完了ならば、再び初期化コマンドの送信をおこなう（７０３）。ＭＭＣ１１０の初期化が完了したならば、ホスト機器２２０は、ＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した標準メモリカードコマンド（フラッシュメモリチップ１３０へアクセスするためのコマンド）や、上に述べたセキュリティ処理に関連した特定のメモリカードコマンド（ＩＣカードチップ１５０へアクセスするためのコマンド）の送信を待機する状態に移る（７０７）。この待機状態では、ホスト機器２２０は標準メモリカードコマンドを送信することができる（７０８）。ＭＭＣ１１０が標準メモリカードコマンドを受信したら、ＭＭＣ１１０はそれを処理する（７０９）。処理が完了したら、ホスト機器２２０は、再び待機状態にもどる（７０７）。

【００５７】この待機状態では、ホスト機器２２０はセキュリティ処理要求ライトコマンドを送信することもできる（７１０）。セキュリティ処理要求ライトコマンドとは、上に述べたセキュリティ処理に関連した特定のメモリカードコマンドの１種であり、ＭＭＣ１１０にセキュリティ処理を実行させるために処理要求を送信するメモリカードコマンドである。ＭＭＣ１１０がセキュリティ処理要求ライトコマンドを受信したら、ＣＰＵ１２１は、要求されたセキュリティ処理の内容を解釈し、セキュリティ処理をＩＣカードコマンドの形式で記述する

（７１１）。即ち、ＣＰＵ１２１は、予め定められたルールに従って、ホスト機器２３０からの標準メモリカードコマンドを、ＩＣカードチップ１５０が解釈可能な特定のメモリカードコマンドへ変換する。そして、その結果として得られたＩＣカードコマンドをＩＣカードチップ１５０に発行するなどして、要求されたセキュリティ処理を実行する（７１２）。処理が完了したら、ホスト機器２２０は、再び待機状態にもどる（７０７）。この待機状態では、ホスト機器２２０はセキュリティ処理結果リードコマンドを送信することもできる（７１３）。セキュリティ処理結果リードコマンドとは、上に述べたセキュリティ処理に関連した特定のメモリカードコマンドの１種であり、ＭＭＣ１１０によるセキュリティ処理の実行結果を知るために処理結果を受信するメモリカードコマンドである。ＭＭＣ１１０がセキュリティ処理結果リードコマンドを受信したら、ＣＰＵ１２１は、ＩＣカードチップ１５０から受信したＩＣカードレスポンスをベースに、ホスト機器２２０に送信すべきセキュリティ処理結果を構築する（７１４）。そして、ホスト機器２２０は、ＭＭＣ１１０からセキュリティ処理結果を受信する。受信が完了したら、ホスト機器２２０は、再び待機状態にもどる（７０７）。なお、ステップ７１４は、ステップ７１２の中でおこなってもよい。

【００５８】図７において、ステップ７０２およびステップ７０５で実行する第１次ＩＣカード初期化処理および第２次ＩＣカード初期化処理は、ＭＭＣ１１０内でセキュリティ処理を実行するのに備えて、ＣＰＵ１２１がＩＣカードチップ１５０に対してアクセスする処理である。具体的には、ＩＣカードチップ１５０の活性化や非活性化、ＩＣカードチップ１５０のリセット、ＩＣカードチップ１５０の環境設定を行う。環境設定とは、セキュリティ処理を実行するために必要な情報（例えば、使用可能な暗号アルゴリズムの情報、暗号計算に使用する秘密鍵や公開鍵に関する情報、個人認証に使用する認証データに関する情報など）をＩＣカードチップ１５０から読み出したり、あるいはＩＣカードチップ１５０に書き込んだりすることを意味する。ＩＣカードチップ１５０の環境設定は、ＩＣカードチップ１５０にＩＣカードコマンドをＮ個（Ｎは正の整数）発行することによっておこなう。例えば、セッション鍵が３個必要ならば、ＩＣカードコマンドを３回発行し、セッション鍵が２個必要ならば、ＩＣカードコマンドを２回発行する。Ｎ個のＩＣカードコマンドは、互いに相違するものであってもよいし、同一のものであってもよい。Ｎの値は固定されたものではなく、状況によってさまざまな値となる。以下、環境設定で発行するＩＣカードコマンドを、設定コマンドと呼ぶ。また、この環境設定に基づいてセキュリティ処理を実行するＩＣカードコマンドを、以下、セキュリティコマンドと呼ぶ。セキュリティコマンドの例としては、デジタル署名の計算、デジタル署名の検証、メッセージの暗号化、暗号化メッセージの復号、パスワードによる認証などをおこなうコマンドがある。

【００５９】ＣＰＵ１２１は、ＩＣカードチップ１５０の環境設定の内容を自由に変更することができる。ＣＰＵ１２１は、セキュリティ処理の内容や結果に応じてこれを変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機としてこれを変更してもよい。また、ＣＰＵ１２１は、環境設定の内容を示した情報をフラッシュメモリチップ１３０にライトし、必要なときにフラッシュメモリチップ１３０からその情報をリードして使用することもできる。この情報は、図２１においてＩＣカード環境設定情報２１１２として示されている。これにより、ＭＭＣ１１０が非活性化されてもその情報を保持することができ、ＭＭＣ１１０が活性化されるたびにあらためて設定する手間を省くことができる。

【００６０】第１次ＩＣカード初期化処理および第２次ＩＣカード初期化処理は、ＩＣカード制御パラメータＡ、Ｂ、Ｃに設定された値に基づいておこなわれる。また、ＣＰＵ１２１は、ステップ７１２で実行するセキュリティ処理において、ＩＣカード制御パラメータＤに設定された値に基づいてＩＣカードチップ１５０の活性化や非活性化を制御する。

【００６１】図８は、ＩＣカード制御パラメータの種類と設定値、それに対応した処理の内容を表している。まず、パラメータＡは、ＭＭＣ１１０に電源が供給されたときに実行される第１次ＩＣカード初期化処理に関するパラメータである。Ａ＝０のときは、ＣＰＵ１２１はＩＣカードチップ１５０にアクセスしない。Ａ＝１のときは、ＣＰＵ１２１はＩＣカードチップ１５０をコールドリセットする。Ａ＝２のときは、ＣＰＵ１２１はＩＣカードチップ１５０をコールドリセットした後でＩＣカードチップ１５０の環境設定をおこなう。Ａ＝３のときは、ＣＰＵ１２１はＩＣカードチップ１５０をコールドリセットした後でＩＣカードチップ１５０の環境設定をおこない、最後にＩＣカードチップ１５０を非活性化する。Ａ＝０またはＡ＝３のときは、第１次ＩＣカード初期化処理のあとＩＣカードチップ１５０が非活性状態となる。Ａ＝１またはＡ＝２のときは、第１次ＩＣカード初期化処理のあとＩＣカードチップ１５０は活性状態となる。

【００６２】次に、パラメータＢとＣは、ＭＭＣ１１０がＭＭＣ初期化コマンドを処理したときに実行される第２次ＩＣカード初期化処理に関するパラメータである。Ｂ＝０のときは、ＣＰＵ１２１はＩＣカードチップ１５０にアクセスしない。Ｂ＝１かつＣ＝１のときは、ＣＰＵ１２１はＩＣカードチップ１５０をリセット（コールドリセットまたはウォームリセット）する。Ｂ＝１かつＣ＝２のときは、ＣＰＵ１２１はＩＣカードチップ１５０をリセットした後でＩＣカードチップ１５０の環境設定をおこなう。Ｂ＝１かつＣ＝３のときは、ＣＰＵ１２

１はＩＣカードチップ１５０をリセットした後でＩＣカードチップ１５０の環境設定をおこない、最後にＩＣカードチップ１５０を非活性化する。Ｂ＝２かつＣ＝２のときは、ＣＰＵ１２１はＩＣカードチップ１５０の環境設定をおこなう。Ｂ＝２かつＣ＝３のときは、ＣＰＵ１２１はＩＣカードチップ１５０の環境設定をおこなった後にＩＣカードチップ１５０を非活性化する。Ｂ＝３のときは、ＩＣカードチップ１５０が活性状態ならば、ＣＰＵ１２１はＩＣカードチップ１５０を非活性化する。最後に、パラメータＤは、ホスト機器２２０から要求されたセキュリティ処理を実行したあとに、ＩＣカードチップ１５０を非活性化するか否かを示すパラメータである。Ｄ＝０のときは、セキュリティ処理の実行後に、ＣＰＵ１２１はＩＣカードチップ１５０を非活性化せず、活性状態に保つ。Ｄ＝１のときは、セキュリティ処理の実行後に、ＣＰＵ１２１はＩＣカードチップ１５０を非活性化する。

【００６３】ＣＰＵ１２１は、ＩＣカード制御パラメータＡ、Ｂ、Ｃ、Ｄの設定値を変更することができる。ＣＰＵ１２１は、セキュリティ処理の内容や結果に応じてこれらの設定値を変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機としてこれらの設定値を変更してもよい。また、ＣＰＵ１２１は、これらの設定値をフラッシュメモリチップ１３０にライトし、必要なときにフラッシュメモリチップ１３０からこれらの設定値をリードして使用することもできる。これらの設定値は、図２１においてＩＣカード制御パラメータ２１１１として示されている。これにより、ＭＭＣ１１０が非活性化されてもこれらの設定値を保持することができ、ＭＭＣ１１０が活性化されるたびにあらためて設定する手間を省くことができる。

【００６４】図９は、第１次ＩＣカード初期化処理のフローチャートを表している。初期化処理を開始する（９０１）と、まず、ＩＣカード制御パラメータＡが０かチェックする（９０２）。Ａ＝０ならばそのまま初期化処理は終了する（９０８）。Ａ＝０でないならばＩＣカードチップ１５０をコールドリセットする（９０３）。次に、ＩＣカード制御パラメータＡが１かチェックする（９０４）。Ａ＝１ならば初期化処理は終了する（９０８）。Ａ＝１でないならばＩＣカードチップ１５０の環境設定をおこなう（９０５）。次に、ＩＣカード制御パラメータＡが２かチェックする（９０６）。Ａ＝２ならば初期化処理は終了する（９０８）。Ａ＝２でないならばＩＣカードチップ１５０を非活性化する（９０７）。そして、初期化処理は終了する（９０８）。

【００６５】図１０は、第２次ＩＣカード初期化処理のフローチャートを表している。初期化処理を開始する（１００１）と、まず、ＩＣカード制御パラメータＢが０かチェックする（１００２）。Ｂ＝０ならばそのまま初期化処理は終了する（１０１３）。Ｂ＝０でないならばＢ＝１かチェックする（１００３）。Ｂ＝１ならばＩＣカード制御パラメータＡが０または３かチェックする（１００４）。Ａが０または３ならば、ＩＣカードチップ１５０をコールドリセットし（１００５）、ステップ１００７に移る。Ａが１または２ならば、ＩＣカードチップ１５０をウォームリセットし（１００６）、ステップ１００７に移る。ステップ１００７では、ＩＣカード制御パラメータＣが１かチェックする。Ｃ＝１ならば初期化処理は終了する（１０１３）。Ｃ＝１でないならばステップ１００９に移る。ステップ１００３においてＢ＝１でないならば、Ｂが２かチェックする（１００８）。Ｂ＝２ならばステップ１００９に移る。Ｂ＝２でないならば、ＩＣカード制御パラメータＡが０または３かチェックする（１０１１）。Ａが０または３ならば初期化処理を終了する（１０１３）。Ａが１または２ならば、ステップ１０１２に移る。ステップ１００９ではＩＣカードチップ１５０の環境設定をおこなう。そして、ＩＣカード制御パラメータＣが２かチェックする（１０１０）。Ｃ＝２ならば初期化処理を終了する（１０１３）。Ｃ＝２でないならばステップ１０１２に移る。ステップ１０１２ではＩＣカードチップ１５０を非活性化する。そして、初期化処理を終了する（１０１３）。

【００６６】図１１は、ＩＣカードチップ１５０が非活性状態であるときに第１次ＩＣカード初期化処理あるいは第２次ＩＣカード初期化処理を実行した場合において、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図１２は、ＩＣカードチップ１５０が活性状態であるときに第２次ＩＣカード初期化処理を実行した場合において、ＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図１１と図１２において、時間の方向は左から右にとっており、上の行から下の行に向かってＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、Ｉ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。図１１において１１０２は図３に示したコールドリセットの信号波形を表す。図１２において１２０２は図４に示したウォームリセットの信号波形を表す。図１１と図１２において、第１設定コマンド処理１１０４ａと１２０４ａ、第２設定コマンド処理１１０４ｂと１２０４ｂ、第Ｎ設定コマンド処理１１０４ｃと１２０４ｃは、それぞれ図５に示したＩＣカードコマンド処理の信号波形を表す。ＩＣカードチップ１５０の環境設定の信号波形１１０４と１２０４は、Ｎ個の設定コマンド処理の信号波形が連なって構成される。図１１と図１２において、１１０６と１２０６は、それぞれ図６に示した非活性化の信号波形を表す。図１１と図１２において、縦方向の破線１１０１、１１０３、１１０５、１１０７、１２０１、１２０３、１２０５、１２０７はそれぞれ特定の時刻を表す。１１０１はコールドリセット前の時刻、１２０１

はウォームリセット前の時刻、１１０３はコールドリセット後から環境設定前の間にある時刻、１２０３はウォームリセット後から環境設定前の間にある時刻、１１０５と１２０５は環境設定後から非活性化前の間にある時刻、１１０７と１２０７は非活性化後の時刻である。

【００６７】図１１を参照して、第１次ＩＣカード初期化処理実行時の信号波形を示す。ＩＣカード制御パラメータＡが０のときは、信号波形に変化はない。Ａ＝１のときは、時刻１１０１から時刻１１０３までの範囲の信号波形となる。Ａ＝２のときは、時刻１１０１から時刻１１０５までの範囲の信号波形となる。Ａ＝３のときは、時刻１１０１から時刻１１０７までの範囲の信号波形となる。

【００６８】図１１を参照して、ＩＣカード制御パラメータＡが０または３のときの、第２次ＩＣカード初期化処理実行時の信号波形を示す。ＩＣカード制御パラメータＢが０のときは、信号波形に変化はない。Ｂ＝１かつＩＣカード制御パラメータＣ＝１のときは、時刻１１０１から時刻１１０３までの範囲の信号波形となる。Ｂ＝１かつＣ＝２のときは、時刻１１０１から時刻１１０５までの範囲の信号波形となる。Ｂ＝１かつＣ＝３のときは、時刻１１０１から時刻１１０７までの範囲の信号波形となる。

【００６９】図１２を参照して、ＩＣカード制御パラメータＡが１または２のときの、第２次ＩＣカード初期化処理実行時の信号波形を示す。ＩＣカード制御パラメータＢが０のときは、信号波形に変化はない。Ｂ＝１かつＩＣカード制御パラメータＣ＝１のときは、時刻１２０１から時刻１２０３までの範囲の信号波形となる。Ｂ＝１かつＣ＝２のときは、時刻１２０１から時刻１２０５までの範囲の信号波形となる。Ｂ＝１かつＣ＝３のときは、時刻１２０１から時刻１２０７までの範囲の信号波形となる。Ｂ＝２かつＣ＝２のときは、時刻１２０３から時刻１２０５までの範囲の信号波形となる。Ｂ＝２かつＣ＝３のときは、時刻１２０３から時刻１２０７までの範囲の信号波形となる。Ｂ＝３のときは、時刻１２０５から時刻１２０７までの範囲の信号波形となる。

【００７０】図１３は、図７のステップ７１２において、ＣＰＵ１２１が、ホスト機器２２０が要求したセキュリティ処理をＩＣカードチップ１５０によって実行するときのフローチャートを表している。セキュリティ処理を開始する（１３０１）と、まずＩＣカードチップ１５０が非活性状態かをチェックする（１３０２）。非活性状態ならば、ＩＣカードチップ１５０をコールドリセットし（１３０３）、ステップ１３０６に移る。活性状態ならば、ステップ１３０４に移る。ステップ１３０４では、ＩＣカードチップ１５０にＩＣカードコマンドを発行する前にＩＣカードチップ１５０を再リセットする必要があるかをチェックする。必要があるならば、ＩＣカードチップ１５０をウォームリセットし（１３０５）、ステップ１３０６に移る。必要がないならば、ステップ１３０６に移る。ステップ１３０６では、ＩＣカードチップ１５０の環境設定をおこなう必要があるかをチェックする。必要があるならば、ＩＣカードチップ１５０の環境設定をおこない（１３０７）、ステップ１３０８に移る。必要がないならば、ステップ１３０８に移る。ステップ１３０８では、ＩＣカードチップ１５０のＣＬＫ２端子に供給するクロック信号の周波数Ｆ２を設定する。そして、ＣＰＵ１２１はＩＣカードチップ１５０にセキュリティコマンドを発行し、ＩＣカードチップ１５０はそれを処理する（１３０９）。セキュリティコマンドの処理時間は、クロック周波数Ｆ２に依存する。

【００７１】次に、ＩＣカードチップ１５０が出力するＩＣカードレスポンスにより、その処理が成功したかどうかを判定する（１３１０）。成功ならば、ステップ１３１１に移る。失敗ならば、ステップ１３１２に移る。ステップ１３１１では、ＩＣカードチップ１５０に発行すべきセキュリティコマンドが全て完了したかをチェックする。発行すべきセキュリティコマンドがまだあるならば、ステップ１３０４に移る。発行すべきセキュリティコマンドが全て完了したならば、ステップ１３１４に移る。ステップ１３１２では、失敗したセキュリティコマンドをリトライすることが可能かを判定する。リトライできるなら、リトライ設定をおこない（１３１３）、ステップ１３０４に移る。リトライ設定とは、リトライすべきセキュリティコマンドやその関連データをＣＰＵ１２１が再度準備することである。リトライできないならステップ１３１４に移る。これは、ホスト機器２２０が要求したセキュリティ処理が失敗したことを意味する。ステップ１３１４では、ＩＣカード制御パラメータＤをチェックする。Ｄ＝１ならば、ＩＣカードチップ１５０を非活性化して（１３１５）、セキュリティ処理を終了する（１３１６）。Ｄ＝１でないならば、ＩＣカードチップ１５０を活性状態に保ったままセキュリティ処理を終了する（１３１６）。図１３のフローチャートにおいては、クロック周波数Ｆ２を、ステップ１３０９で発行するセキュリティコマンドの種類によって変えることができるように、ステップ１３０８をステップ１３０９の直前に位置させたが、ステップ１３０８はそれ以外の位置にあってもよい。

【００７２】従来のＩＣカードへの攻撃法を有効にしている要因のひとつとして、ＩＣカードの駆動クロックが外部の接続装置から直接供給されることがあげられる。駆動クロックが接続装置の制御下にあるため、タイミング解析や電力差分解析においては、電気信号の測定においてＩＣカード内部処理のタイミングの獲得が容易になる。一方、故障利用解析においては、異常な駆動クロックの供給による演算エラーの発生が容易になる。これに対し、本発明によれば、ＭＭＣ１１０内部でＩＣカードチップ１５０によりセキュリティ処理を実行するとき、

ホスト機器２２０はＩＣカードチップ１５０の駆動クロックを直接供給できない。ＣＰＵ１２１は、ＩＣカードチップ１５０へ供給するクロックの周波数Ｆ２を自由に設定することができる。これにより、ホスト機器２２０の要求する処理性能に柔軟に対応したセキュリティ処理が実現できる。ホスト機器２２０が高速なセキュリティ処理を要求するならば周波数Ｆ２を高く設定し、低い消費電力を要求するならば周波数Ｆ２を低く設定したり、クロックを適度に停止させればよい。

【００７３】また、ＣＰＵ１２１は、周波数Ｆ２だけでなくクロックの供給開始タイミング、供給停止タイミングを自由に設定できる。これらをランダムに変化させることにより、ＩＣカードチップ１５０に対するタイミング解析、電力差分解析、故障利用解析と呼ばれる攻撃法を困難にすることができる。タイミング解析は、攻撃者が暗号処理１回の処理時間を正確に計測可能であることを仮定しているため、その対策としては、攻撃者が処理時間計測を正確に行えないようにすることが有効である。本発明によりタイミング解析が困難になる理由は、ＩＣカードチップ１５０がＩＣカードコマンドを処理している時間の長さをホスト機器２２０が正確に計測できないためである。電力差分解析の対策としては、処理の実行タイミングや順序に関する情報を外部から検出不可能にすることが有効である。本発明により電力差分解析が困難になる理由は、ＩＣカードコマンドが発行された時刻、発行されたＩＣカードコマンドの内容、発行されたＩＣカードコマンドの順序（ＩＣカードコマンドを複数組み合わせてセキュリティ処理を実行する場合）の検出がホスト機器２２０にとって困難になるためである。

【００７４】故障利用解析の対策としては、ＩＣカードにクロックや電圧や温度等の動作環境検知回路を搭載し、異常を検出したならば処理を停止あるいは使用不能にするという方法が有効である。本発明により故障利用解析が困難になる理由は、ＣＬＫ２制御回路１２７がＩＣカードチップ１５０に異常な駆動クロックを供給しないことが、ホスト機器２２０がＩＣカードチップ１５０に演算エラーを発生させるのを防止するからである。

【００７５】ＣＰＵ１２１は、ＩＣカードチップ１５０に供給するクロックの周波数Ｆ２、供給開始タイミング、供給停止タイミングの設定値を、セキュリティ処理の内容や結果に応じて変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機として変更してもよい。また、ＣＰＵ１２１は、これらの設定値をフラッシュメモリチップ１３０にライトし、必要なときにフラッシュメモリチップ１３０からこれらの設定値をリードして使用することもできる。これらの設定値は、図２１においてＣＬＫ２設定情報２１１３として示されている。これにより、ＭＭＣ１１０が非活性化されてもこれらの設定値を保持することができ、ＭＭＣ１１０が活性化されるたびにあらためて設定する手間を省くことができる。

【００７６】図１４は、ホスト機器２２０がセキュリティ処理要求ライトコマンドをＭＭＣ１１０に発行してから、ＩＣカードチップ１５０でセキュリティ処理が実行されるまでの過程（図７のステップ７１０～７１２）において、ＭＭＣ１１０およびＩＣカードチップ１５０の外部端子の信号波形、ＣＰＵ１２１によるフラッシュメモリチップ１３０へのアクセスをシンプルに表したものである。図１４において、時間の方向は左から右にとる。

【００７７】一番上の行はフラッシュメモリチップ１３０へのアクセス内容である。上から二行目の行から下の行に向かって、ＶＣＣ１端子１４４、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、ＤＡＴ端子１４７、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、Ｉ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。図１４を参照して、ホスト機器２２０がセキュリティ処理要求ライトコマンドをＭＭＣ１１０に発行してから、ＩＣカードチップ１５０でセキュリティ処理が実行されるまでの過程を説明する。

【００７８】まず、ホスト機器２２０はＣＭＤ端子１４２にセキュリティ処理要求ライトコマンドを送信する（１４０１）。次に、ホスト機器２２０はＣＭＤ端子１４２からセキュリティ処理要求ライトコマンドのレスポンスを受信する（１４０２）。このレスポンスは、ＭＭＣ１１０がコマンドを受信したことをホスト機器２２０に伝えるものであり、セキュリティ処理の実行結果ではない。次に、ホスト機器２２０はＤＡＴ端子１４７にセキュリティ処理要求を送信する（１４０３）。セキュリティ処理要求とは、セキュリティ処理の内容や処理すべきデータを含むホストデータである。次に、ＭＭＣ１１０はＤＡＴ端子１４７をＬレベルにセットする（１４０４）。ＭＭＣ１１０は、これによりビジー状態であることをホスト機器２２０に示す。次に、ＣＰＵ１２１は、ホスト機器２２０から受信したセキュリティ処理要求をフラッシュメモリチップ１３０にライトするコマンドを発行する（１４０５）。セキュリティ処理要求をフラッシュメモリチップ１３０にライトすることにより、ＣＰＵ１２１がセキュリティ処理要求をＩＣカードコマンド形式で記述する処理（図７のステップ７１１）において、ＣＰＵ１２１内部のワークメモリの消費量を節約できる。これは、セキュリティ処理要求のデータサイズが大きいときに有効である。

【００７９】なお、フラッシュメモリチップ１３０にライトされたセキュリティ処理要求は、図２１においてセキュリティ処理バッファ領域２１１４に格納される。また、ライトコマンド発行１４０５は必須な操作ではない。ライト処理期間１４０６は、フラッシュメモリチップ１３０がセキュリティ処理要求のライト処理を実行し

ている期間を表す。セキュリティ処理１４０７はＩＣカードチップ１５０によるセキュリティ処理の信号波形を表す。この信号波形は図１３のフローチャートの遷移過程に依存する。セキュリティ処理１４０７は、ライト処理期間１４０６とオーバラップさせることができる。一般にフラッシュメモリチップ１３０のライト処理期間１４０６はミリ秒のオーダーであるため、セキュリティ処理１４０７とオーバラップさせることは、セキュリティ処理の全体的な処理時間の短縮にとって有効である。

【００８０】リード／ライト１４０８は、セキュリティ処理１４０７の実行中に、フラッシュメモリチップ１３０からセキュリティ処理要求をリードしたり、ＩＣカードチップ１５０が出力した計算結果をフラッシュメモリチップ１３０にライトするアクセスを示している。このアクセスにより、ＣＰＵ１２１内部のワークメモリの消費量を節約できる。これは、セキュリティ処理要求やセキュリティ処理結果のデータサイズが大きいときに有効である。リード／ライト１４０８は必須ではない。セキュリティ処理１４０７が完了したら、ＭＭＣ１１０はＤＡＴ端子１４７をＨレベルにセットする（１４０９）。ＭＭＣ１１０は、これによりセキュリティ処理が完了したことをホスト機器２２０に示す。

【００８１】図１５は、図１４におけるセキュリティ処理１４０７の信号波形の一例を表したものである。図１５において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ１３０へのアクセス内容である。上から二行目の行から下の行に向かって、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、Ｉ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。１５０１は図３に示したコールドリセットの信号波形を表し、１５０４は図４に示したウォームリセットの信号波形を表し、１５０２および１５０５は図１１（あるいは図１２）に示した環境設定の信号波形を表し、１５０３および１５０６および１５０７は図５に示したＩＣカードコマンド処理の信号波形を表し、１５０８は図６に示した非活性化の信号波形を表す。ＩＣカードチップ１５０の外部端子において図１５に示した信号波形が観測されるのは、図１３のフローチャートが１３０１、１３０２、１３０３、１３０６、１３０７、１３０８、１３０９、１３１０、１３１１、１３０４、１３０５、１３０６、１３０７、１３０８、１３０９、１３１０、１３１１、１３０４、１３０６、１３０８、１３０９、１３１０、１３１１、１３１４、１３１５、１３１６の順で遷移するときである。

【００８２】図１５を参照して、図１４のセキュリティ処理１４０７の実行中におけるＣＰＵ１２１によるフラッシュメモリチップ１３０へのアクセス（リード／ライト１４０８）を説明する。このアクセスには、図２１におけるセキュリティ処理バッファ領域２１１４を使用する。リード１５０９、１５１１、１５１２は、それぞれ、セキュリティコマンド処理１５０３、１５０６、１５０７においてＩＣカードチップ１５０に送信するＩＣカードコマンドを構築するために必要なデータを、フラッシュメモリチップ１３０からリードするアクセスである。ライト１５１０は、セキュリティコマンド処理１５０３においてＩＣカードチップ１５０が出力した計算結果を、フラッシュメモリチップ１３０にライトするアクセスである。ライト１５１３は、セキュリティコマンド処理１５０６および１５０７においてＩＣカードチップ１５０が出力した計算結果を、フラッシュメモリチップ１３０にまとめてライトするアクセスである。リード１５０９、１５１１、１５１２は、それぞれ、セキュリティコマンド処理１５０３、１５０６、１５０７以前のＩＣカードチップ１５０へのアクセスとオーバラップさせることができる。ライト１５１０、１５１３は、それぞれ、セキュリティコマンド処理１５０３、１５０７以後のＩＣカードチップ１５０へのアクセスとオーバラップさせることができる。これらのオーバラップは、セキュリティ処理の全体的な処理時間の短縮にとって有効である。

【００８３】さらに、フラッシュメモリチップ１３０のライト単位が大きい場合は、ライト１５１３のように複数の計算結果をまとめてライトすることができる。これは、フラッシュメモリチップ１３０へのライト回数を削減し、フラッシュメモリチップ１３０の劣化を遅らせる効果がある。なお、ライト１５１０、１５１３でフラッシュメモリチップ１３０にライトする内容は、ＩＣカードチップ１５０が出力した計算結果そのものに限定されず、図７のステップ７１５でホスト機器２２０に返すセキュリティ処理結果またはその一部であってもよい。この場合、図７のステップ７１４またはその一部は、ステップ７１２の中で実行されることになる。

【００８４】図１６は、ホスト機器２２０がセキュリティ処理結果リードコマンドをＭＭＣ１１０に発行してから、ＭＭＣ１１０がセキュリティ処理結果を出力するまでの過程（図７のステップ７１３～７１５）において、ＭＭＣ１１０の外部端子の信号波形、ＣＰＵ１２１によるフラッシュメモリチップ１３０へのアクセスをシンプルに表したものである。図１６において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ１３０へのアクセス内容である。上から二行目の行から下の行に向かって、ＶＣＣ１端子１４４、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、ＤＡＴ端子１４７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。

【００８５】図１６を参照して、ホスト機器２２０がセキュリティ処理結果リードコマンドをＭＭＣ１１０に発行してから、ＭＭＣ１１０がセキュリティ処理結果を出力するまでの過程を説明する。まず、ホスト機器２２０

はＣＭＤ端子１４２にセキュリティ処理結果リードコマンドを送信する（１６０１）。次に、ホスト機器２２０はＣＭＤ端子１４２からセキュリティ処理結果リードコマンドのレスポンスを受信する（１６０２）。このレスポンスは、ＭＭＣ１１０がコマンドを受信したことをホスト機器２２０に伝えるものであり、セキュリティ処理結果ではない。次に、ＭＭＣ１１０はＤＡＴ端子１４７をＬレベルにセットする（１６０３）。ＭＭＣ１１０は、これによりビジー状態であることをホスト機器２２０に示す。次に、ＣＰＵ１２１は、フラッシュメモリチップ１３０のセキュリティ処理バッファ領域（図２１の２１１４）から、ＩＣカードチップ１５０が出力した計算結果をリードする（１６０４）。ＣＰＵ１２１は、これをもとにセキュリティ処理結果を構築し、ＭＭＣ１１０がＤＡＴ端子１４７にセキュリティ処理結果を出力する（１６０５）。

【００８６】なお、図７のステップ７１４またはその一部が、ステップ７１２の中で実行されている場合、ステップ１６０４ではフラッシュメモリチップ１３０のセキュリティ処理バッファ領域（図２１の２１１４）からセキュリティ処理結果またはその一部をリードする。なお、フラッシュメモリチップ１３０のセキュリティ処理バッファ領域（図２１の２１１４）を利用しないでセキュリティ処理結果を構築する場合、ステップ１６０４は必要ない。

【００８７】ＭＭＣ１１０の製造者や管理者は、セキュリティシステムのユーザにＭＭＣ１１０を提供する前やそのユーザが所有するＭＭＣ１１０に問題が発生した時に、ＭＭＣ１１０に内蔵されたＩＣカードチップ１５０に様々な初期データを書きこんだり、ＩＣカードチップ１５０のテストをおこなったりする必要がある。ＭＭＣ１１０の製造者や管理者によるこれらの操作の利便性を高めるために、ＭＭＣ１１０は、ＩＣカードチップ１５０の外部端子をＭＭＣ外部端子１４０に割りつけるインタフェース機能を持つ。これにより、図３～図６で示したようなＩＣカードチップ１５０へのアクセス信号を、ＭＭＣ外部端子１４０から直接送受信できる。このようなＭＭＣ１１０の動作モードを、ＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した動作モードと区別して、以下、インタフェース直通モードと呼ぶ。

【００８８】インタフェース直通モードについて詳細に説明する。図１７は、ＩＣカードチップ１５０の外部端子をＭＭＣ外部端子１４０に割りつけるときの対応関係の一例を表している。この例では、ＲＳＴ端子１５２をＣＳ端子１４１に割り付け、ＧＮＤ２端子１５５をＧＮＤ１端子１４３、１４６に割り付け、ＶＣＣ２端子１５１をＶＣＣ１端子１４４に割り付け、ＣＬＫ２端子１５３をＣＬＫ１端子１４５に割り付け、Ｉ／Ｏ端子１５７をＤＡＴ端子１４７に割り付ける。このとき、ＣＳ端子１４１とＣＬＫ１端子１４５は入力端子、ＤＡＴ端子１４７は入出力端子として機能する。

【００８９】ＭＭＣ１１０は、特定のメモリカードコマンドを受信すると、動作モードをインタフェース直通モードへ移したり、インタフェース直通モードからＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した動作モードに戻すことができる。以下、動作モードをインタフェース直通モードへ移すメモリカードコマンドを直通化コマンド、動作モードをインタフェース直通モードから通常の状態に戻すメモリカードコマンドを復帰コマンドと呼ぶ。図１を参照して、ＭＭＣＩ／Ｆ制御回路１２３は、ＶＣＣ２制御回路１２６、ＣＬＫ２制御回路１２７、ＩＣカードＩ／Ｆ制御回路１２８と接続されており、ＭＭＣ１１０がホスト機器２２０から直通化コマンドを受信すると、ＣＰＵ１２１の指示により図１７で示した端子割り付けをおこなう。ＭＭＣ１１０がホスト機器２２０から復帰コマンドを受信すると、ＣＰＵ１２１の指示により図１７で示した端子割り付けを解除し、ＭＭＣ１１０はＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した動作モードに戻る。

【００９０】インタフェース直通モードでは、ホスト機器２２０がＩＣカードチップ１５０に直接アクセスできるため、セキュリティの観点からインタフェース直通モードを利用できるのは限られた者だけにする必要がある。そこで、直通化コマンドの発行には、一般のユーザに知られないパスワードの送信を必要とする。正しいパスワードが入力されないとインタフェース直通モードは利用できない。

【００９１】図１８は、ホスト機器２２０が、ＭＭＣ１１０の動作モードをＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した動作モードからインタフェース直通モードに移し、ＩＣカードチップ１５０に直接アクセスし、その後、ＭＭＣ１１０の動作モードを再びＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した動作モードに戻すまでの処理のフローチャートを表している。ホスト機器２２０は処理を開始し（１８０１）、まずＭＭＣ１１０に直通化コマンドを発行する（１８０２）。ＭＭＣ１１０は、直通化コマンドで送信されたパスワードが正しいかチェックする（１８０３）。正しければステップ１８０４に移り、間違っていれば処理は終了する（１８１０）。ステップ１８０４では、ＣＰＵ１２１は、ＩＣカードチップ１５０をコールドリセットする。そして、図１７で示した端子割り付けをおこないインタフェースを直通化する（１８０５）。この時点から、ホスト機器２２０はＩＣカードチップ１５０に直接アクセスする（１８０６）。ホスト機器２２０がＩＣカードチップ１５０への直接アクセスを終了し、ＭＭＣ１１０の動作モードを再びＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した動作モードに戻すときは、ＭＭＣ１１０に復帰コマンドを発行する（１８０７）。すると、ＣＰＵ１２１は図１７で示した端子割り付けを解除し、ＭＭＣ１１０はＭｕｌｔｉＭｅ

ｄｉａＣａｒｄ仕様に準拠した動作モードに戻る（１８０８）。そして、ＣＰＵ１２１は、ＩＣカードチップ１５０を非活性化する（１８０９）。以上で、処理は終了する（１８１０）。

【００９２】図１９は、図１８のステップ１８０１～１８０６の過程において、ＭＭＣ１１０およびＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図１９において、時間の方向は左から右にとる。上の行から下の行に向かって、ＶＣＣ１端子１４４、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、ＤＡＴ端子１４７、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、Ｉ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。１９０５は、図３のコールドリセットの信号波形を示す。モード移行時刻１９０６は、動作モードがインタフェース直通モードに移る時刻を表す。

【００９３】図１９を参照して、ホスト機器２２０がＭＭＣ１１０の動作モードをＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した動作モードからインタフェース直通モードに移しＩＣカードチップ１５０に直接アクセスする過程を説明する。なお、ＭＭＣ１１０のＶＣＣ１端子１４４には３Ｖ（ＶＣＣ２端子１５１の標準電圧）が供給されている。ホスト機器２２０がＣＭＤ端子１４２に直通化コマンドを入力すると（１９０１）、ＣＭＤ端子１４２から直通化コマンドのレスポンスが出力される（１９０２）。このレスポンスは、ＭＭＣ１１０がコマンドを受信したことをホスト機器２２０に伝えるものである。次に、ホスト機器２２０はＤＡＴ端子１４７にパスワードを入力する（１９０３）。パスワード入力後、ＭＭＣ１１０はＤＡＴ端子１４７にＬレベルを出力し（１９０４）、ビジー状態であることをホスト機器２２０に示す。ビジー状態の間に、ＣＰＵ１２１は、ＩＣカードチップ１５０をコールドリセットする（１９０５）。そして、モード移行時刻１９０６において、動作モードをインタフェース直通モードに移す。このときに、ＤＡＴ端子１４７はＬレベルからハイインピーダンス状態になる。これにより、ホスト機器２２０はビジー状態の解除を知ることができる。この時点から、ホスト機器２２０はＩＣカードチップ１５０に直接アクセスする。例えば、ＣＬＫ１端子１４５にクロックを供給すると（１９０７）、ＣＬＫ２端子１５３にそのクロックが供給される（１９０８）。また、ＤＡＴ端子１４７にＩＣカードコマンドを送信すると（１９０９）、Ｉ／Ｏ端子１５７にそのＩＣカードコマンドが送信される（１９１０）。

【００９４】図２０は、図１８のステップ１８０７～１８１０の過程において、ＭＭＣ１１０およびＩＣカードチップ１５０の外部端子の信号波形をシンプルに表したものである。図２０において、時間の方向は左から右にとる。上の行から下の行に向かって、ＶＣＣ１端子１４４、ＣＭＤ端子１４２、ＣＬＫ１端子１４５、ＤＡＴ端子１４７、ＶＣＣ２端子１５１、ＲＳＴ端子１５２、ＣＬＫ２端子１５３、Ｉ／Ｏ端子１５７で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Ｌレベル）を表す。モード復帰時刻２００３は、動作モードがインタフェース直通モードからＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した動作モードに戻る時刻を表す。２００４は、図６の非活性化の信号波形を示す。

【００９５】図２０を参照して、ホスト機器２２０がＭＭＣ１１０の動作モードをインタフェース直通モードからＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した動作モードに戻す過程を説明する。なお、ＭＭＣ１１０のＶＣＣ１端子１４４には３Ｖ（ＶＣＣ２端子１５１の標準電圧）が供給されている。ホスト機器２２０がＣＭＤ端子１４２に復帰コマンドを入力すると（２００１）、ＣＭＤ端子１４２から復帰コマンドのレスポンスが出力される（２００２）。このレスポンスは、ＭＭＣ１１０がコマンドを受信したことをホスト機器２２０に伝えるものである。そして、モード復帰時刻２００３において、ＭＭＣ１１０はＤＡＴ端子１４７にＬレベルを出力してビジー状態であることをホスト機器２２０に示し、それと同時に動作モードをＭｕｌｔｉＭｅｄｉａＣａｒｄ仕様に準拠した動作モードに戻す。ビジー状態の間に、ＣＰＵ１２１は、ＩＣカードチップ１５０を非活性化する（２００４）。そして、ＭＭＣ１１０は、ＤＡＴ端子１４７をハイインピーダンス状態にし（２００５）、復帰コマンドの処理が完了したことをホスト機器２２０に示す。これ以後、ホスト機器２２０はＩＣカードチップ１５０に直接アクセスできない。ホスト機器２２０が、ＣＬＫ１端子１４５にクロックを供給しながらＣＭＤ端子１４２に何らかのメモリカードコマンドを送信した場合、ＩＣカードチップ１５０にそのクロック信号（２００６）は伝わらない。２００１や２００２においてホスト機器２２０がＣＬＫ１端子１４５に供給するクロック信号は、ＩＣカードチップ１５０のＣＬＫ２端子１５３にも伝わるが、ＤＡＴ端子１４７がハイインピーダンス状態であるため、ＩＣカードチップ１５０がＩＣカードコマンドを誤って認識することはない。

【００９６】図２１において、セキュリティ処理ステータス領域２１１６には、ＩＣカードチップ１５０によるセキュリティ処理の進捗状況を示す情報を格納する。ＣＰＵ１２１は、この情報をセキュリティ処理の実行中に更新することができる。例えば、セキュリティ処理の途中でＭＭＣ１１０への電源供給が停止した場合、電源供給再開時にＣＰＵ１２１がこの情報をリードして参照すれば、セキュリティ処理を中断した段階から再開することができる。

【００９７】次に、本発明の他の実施形態について説明する。

【００９８】図２７は、本発明を適用したカード型記憶

装置２７０１の構成を示した図である。記憶装置２７０１は、フラッシュメモリチップ１３０、コントローラチップ１２０、ＩＣカードチップ１５０、モード選択回路２７１０、及びMMC外部端子１４０を有する。モード選択回路２７１０は、モード選択信号２７２０に基づいて、モード選択回路２７１０に接続された入出力バス２７３０及び入出力バス２７４０のうちいずれか一つを選択し、MMC外部端子１４０とコントローラチップ１２０、又はMMC外部端子１４０とＩＣカードチップ１５０とを論理的に接続する機能を持っている。フラッシュメモリチップ１３０、コントローラチップ１２０、ＩＣカードチップ１５０、及びMMC外部端子１４０の各々のモジュールは、図２２で示したMMC１１０の各々のモジュールと同等の機能を有する。

【００９９】カード型記憶装置２７０１は、モード選択信号２７２０の状態に応じて、MMC又はＩＣカードとして動作する。図２８は、モード選択回路２７１０、入出力バス２７３０、入出力バス２７４０、及びMMC外部端子１４０の接続状態を示した図である。モード選択回路２７１０は、MMC外部端子１４０の各々の信号線（１４１、１４２、１４３、１４４、１４５、１４６、１４７）に対応したスイッチ（２７１１、２７１２、２７１３、２７１４、２７１５、２７１６、２７１７）を持っている。各スイッチは、モード選択信号２７２０の状態によりコントローラチップ１２０の入出力バス２７３０、又は、ＩＣカードチップ１５０の入出力バス２７４０のどちらかとMMC外部端子１４０を接続する。例えば、ＣＳ１４１端子は、コントローラチップ１２０の入出力バス２７３０のＣＳ２７３１か、ＩＣカードチップ１５０の入出力バス２７４０のＲＳＴ１５２のどちらかに接続される。

【０１００】ホスト機器２７０２は、例えばＩＣカードに対応した端末（携帯電話、携帯情報端末（ＰＤＡ）、パーソナルコンピュータ、音楽再生（及び録音）装置、カメラ、ビデオカメラ、自動預金預払器（ＡＴＭ）、セットトップボックス（ＳＴＢ）、街角端末、決済端末等）において、既存のシステムを有効に活用しながらカード型記憶装置２７０１をサポートすることができる。

【０１０１】図２９は、ＩＣカード及びカード型記憶装置２７０１に対応したホスト機器２９０１が有するＩＣカード制御に関連するモジュールの構成を示す図である。ホスト機器２９０１は、MMCソケット２９１０、モード検出回路２９３０、ＩＣカード制御回路２９５０、ＶＣＣ２電源２９６０、ＣＬＫ２発信器２９７０、及びＩＣカードスロット２９８０を有する。尚、ＩＣカードスロット２９８０は装備していなくても構わない。MMCソケット２９１０はMMCソケット端子２９２０を有しており、図２８で示したMMC外部端子１４０と接続される。MMCソケット２９１０は、モード検出回路２９３０に対してモード検出信号２９４０を出力する。モード検出回路２９３０は、モード検出信号２９４０の状態により、MMCソケット２９１０に挿入される記憶装置２７０１が、ＩＣカードとして動作するかどうか判定する。ＩＣカードとして動作する場合、モード検出回路２９３０は、ＩＣカード制御回路２９５０、ＶＣＣ２電源２９６０、ＣＬＫ２発信器２９７０の各信号線と、MMCソケット端子２９２０の信号線を適切に接続する。ＩＣカードとして動作しない場合、MMCソケット端子２９２０の信号線は接続されず、ホスト機器２９０１は記憶装置２７０１を認識しないか、又は非対応の記憶装置２７０１が挿入された旨をユーザに通知する等の処理が行われる。

【０１０２】図３０は、記憶装置２７０１がMMCソケット２９１０に挿入された場合の一例を示す図である。MMCソケット２９１０は、スイッチ３０１０及びスイッチ３０２０を備えており、モードの検出を行う。記憶装置２７０１がMMCソケット２９１０に挿入されると、スイッチ３０１０によりその旨が検出され、スイッチ３０２０に伝播される。スイッチ３０２０は、例えば突起型の形状をしており、スイッチ３０１０から伝播された信号に応じて、記憶装置２７０１の側面に押し込まれる。一方、記憶装置２７０１は、側面に凹みがあり、凹みの位置にスイッチ３０２０が挿入される。記憶装置２７０１が有するスイッチ３０３０は、スイッチ３０２０の挿入の状態を検出し、モード選択信号２７２０を生成し、モード選択回路２７１０に出力する。これは例えば、モード選択信号２７２０をＶＣＣと接続し論理値１の状態にすること等で実現できる。

【０１０３】即ち、記憶装置２７０１がＩＣカードモード対応のホスト機器２９０１に挿入された場合はＩＣカードモードが選択され、そうでない場合はMMCモードが選択される。ホスト機器２９０１は、モード判定をスイッチ３０２０で行い、ホスト機器２９０１にＩＣカードインタフェイスに対応した記憶装置２７０１が挿入されたことを示すモード検出信号２９４０を出力する。これは、例えばモード検出信号２９４０をＶＣＣと接続し論理値１の状態にすること等で実現できる。

【０１０４】ここで、側面に凹みの無い記憶装置２７０１をホスト機器２９０１に挿入すると、スイッチ３０２０は挿入されない。つまり、側面に凹みの無い記憶装置２７０１をＩＣカードモードに対応していない記憶装置２７０１とすれば、スイッチ３０１０がオンの状態でかつスイッチ３０２０の状態と対応するモード検出信号２９４０が出力されない場合は、ＩＣカードモードに対応していない記憶装置２７０１がホスト機器２９０１に挿入されていると判断される。したがって、ホスト機器２９０１は、スイッチ３０１０の状態と合わせてＩＣカードモード非対応の記憶装置２７０１が挿入されたと判定する。なお、スイッチ３０１０並びにスイッチ３０２０はバネ等を利用した機械的なスイッチでも良いし、電気

的なスイッチでも良い。

【０１０５】図３１は、記憶装置２７０１における処理手順を示したフローチャートである。記憶装置２７０１がホスト機器２９０１に挿入されると（Ｓ３１０１）、記憶装置２７０１が有するスイッチ３０３０の状態が決まり（Ｓ３１０２）、モード選択信号２７２０が確定する（Ｓ３１０３）。その後、電源端子ＶＣＣ１（１４４）並びにグランド端子ＧＮＤ１（１４３、１４６）が接続され（Ｓ３１０４）、記憶装置２７０１は、モード選択回路２７１０を起動してモード判定を行う（Ｓ３１０５）。ＩＣカードモードである場合（Ｓ３１０６）、モード選択回路２７１０は、ＭＭＣ外部端子１４０とＩＣチップ信号線（２７４０）を接続する（Ｓ３１０８）。ＭＭＣモードである場合（Ｓ３１０７）、モード選択回路２７１０は、ＭＭＣ外部端子１４０とコントローラチップ信号線２７３０を接続する。

【０１０６】上述の実施形態では、一つの記憶装置２７０１で、ＩＣカードモードとＭＭＣモードを使い分ける一例を示した。次に、他の実施形態について述べる。

【０１０７】図３２は、上述のＩＣカードモード及びＭＭＣモードをサポートしたカード型記憶装置３２１０の概観を示す図である。ここでは便宜上、端子が装着されている面をＢ面３２２０、その反対面をＡ面３２１０とする。通常、ユーザがＡ面３２１０とＢ面３２２０を間違えて挿入できないように、ＭＭＣには、逆挿し防止の機能を有する、挿入方向の片端に斜めの切れ込みが入っている。

【０１０８】カード型記憶装置３２１０は、ＭＭＣと同様の切れ込み並びにＭＭＣ外部端子３２３０に加え、その反対側（図では右側）にも同様の切れ込み及びＩＣカード端子３２４０が装備されている。カード型記憶装置３２１０は、ＭＭＣとして使用される場合はＭＭＣの矢印の示す方向（左側）に、ＩＣカードとして使用される場合はＩＣカードの矢印の示す方向（右側）に、各々挿入されることにより両モードに対応することができる。なお、内部回路の構成については図２７において、コントローラチップ１２０の入出力バス２７３０とＭＭＣ外部端子３２３０を、またＩＣチップの入出力バス２７４０とＩＣカード端子３２４０を各々接続すればよい。この場合、モード選択回路２７１０は無くてもよい。

【０１０９】図３３は、カード型記憶装置３３１０において、ＩＣカードモードとＭＭＣモードをサポートする、図３２とは異なる構成を示した図である。カード型記憶装置３３１０の形状はＭＭＣと変わらず、挿入方向の片端に斜めの切れ込みが入っている。本図の構成においては、ＭＭＣ外部端子３２３０及びＩＣカード端子３２４０は、各々Ｂ面３３２０、Ａ面３３１０のカード挿入方向（図中の右側）に配置されている。即ち、ＭＭＣとして使用する場合は、通常のＭＭＣと同様の向きに挿入し、ＩＣカードとして使用する場合は、ＭＭＣとは逆の向きに挿入する。

【０１１０】図３４は、ホスト機器が有するカード型記憶装置３２１０及び３３１０に対応するＭＭＣソケット２９１０の一例を示す図である。（ａ）タイプ３４１０は、ＭＭＣモードのみサポートしているホスト機器２７０２に使用する。この場合、図３２及び図３３で示したカード型記憶装置３２１０及び３３１０をＩＣカードとして挿入しようとしても、ソケット側の斜めの切れ込みにより、逆挿し防止の機能が働いてカード型記憶装置３２１０及び３３１０を挿入することはできない。（ｂ）タイプ３４２０は、ＩＣカードモードのみサポートしているホスト機器２７０２に使用する。この場合、（ａ）タイプ３４１０とは逆に、ＭＭＣとして挿入しようとしても、切れ込みにより逆挿し防止の機能が働いてカード型記憶装置３２１０及び３３１０を挿入することはできない。（ｃ）タイプ３４３０は、ＩＣカードモード及びＭＭＣモードの両方をサポートするホスト機器２９０１に装着する。両モードの判別は、例えば、スイッチ３４３１を用いて行う。（ｃ）タイプ３４３０のソケットにカード型記憶装置３２１０及び３３１０がＭＭＣとして挿入された場合、カード型記憶装置３２１０及び３３１０が有する斜めの切れ込み部分とスイッチ３４３１の位置が対応し、スイッチ３４３１は作動しない。一方、カード型記憶装置３２１０及び３３１０がＩＣカードとして挿入された場合、カード型記憶装置３２１０及び３３１０の斜めの切れ込み部分がスイッチ３４３１の位置と対応しないため、カード型記憶装置３２１０及び３３１０の角部分がスイッチ３４３１をカード型記憶装置３２１０及び３３１０の挿入方向に押し付ける。これにより、スイッチ３４３１がＯＮとなる。スイッチ３４３１がＯＮになった場合、ＭＭＣソケット２９０１の（ｃ）タイプ３４３０は、挿入されたカード型記憶装置３２１０及び３３１０がＩＣカードとして動作することを判別し、ホスト機器２７０２にその旨を伝える。

【０１１１】上述した実施形態では、カード型記憶装置３２１０及び３３１０の挿入によってＩＣカードモードとＭＭＣモードを判別する例を示したが、モードの判別方法は上述の実施形態だけに限らない。

【０１１２】図３５は、カード型記憶装置３５０１が手動で動作するスイッチ３５１０を有する例を示して図である。ユーザは、自分の使用目的に応じてスイッチ３５１０を切り替えることによりＩＣカードモードとＭＭＣモードを使い分ける。なお、図３５では、スイッチ３５１０はカード型記憶装置３５０１の側面に配置されているが、いずれの面、例えば、正面又は裏面に配置してもよい。

【０１１３】以上述べたように、本実施形態では、カード型記憶装置においてＩＣカードモードとＭＭＣモードをサポートし、その判別を適切に行うことにより各々のモードの処理を実行することが可能である。更に本発明

は、ＩＣカードモードとＭＭＣモードに限らず、様々な動作モードにおいて適用することができる。

【０１１４】図３６は、２系統のモードをサポートするカード型記憶装置３６１０の内部構成を示した図である。カード型記憶装置３６１０は、フラッシュメモリチップ１３０、コントローラチップＡ３６２０、コントローラチップＢ３６３０、モード選択回路３６４０、及び外部端子３６７０を有する。カード型記憶装置３６０１の基本要素は、図２７に示した内部構成とほぼ変わらない。コントローラチップＡ３６２０及びＢ３６３０は、様々なインタフェース制御に適用することができる。例えば、コントローラチップＡ３６２０及びＢ３６３０は、前述のＭＭＣコントローラチップ１２０（図２２）、ＳＤカードコントローラチップ２４２０（図２４）、メモリースティックコントローラチップ２５２０（図２５）に適用することでき、一つのカード型記憶装置で上記複数のメモリカードに対応することが可能となる。

【０１１５】また、カード型記憶装置３６１０は、２系統のモードだけでなく、３系統以上のモードにも容易に拡張できることができる。その場合、外部端子３６７０は、カード型記憶装置３６１０がサポートするインタフェースのうち、そのインタフェースが使用する端子数が最大のもの、又はそれ以上の端子数を有するように構成する。例えば、ＭＭＣとＳＤカードをサポートする場合は９本、ＭＭＣとメモリースティックをサポートする場合は１０本の端子を備える。

【０１１６】モードの切り替え及びモードの判別方法には、前述のようにモード選択信号２７２０を用いる。勿論、前述のインタフェース直通モードの説明（図１７、図１８、図１９、図２０）で述べたように、インターフェースモードをメモリカードのコマンドで切り替える方法も適用できる。前述の例で言えば、インタフェース直通モードへ移すメモリカードコマンド（直通化コマンド）が発行されると、コントローラチップＢ３６３０で制御されるインターフェースモードに移行し、インタフェース直通モードから通常の状態に戻すメモリカードコマンド（復帰コマンド）が発行されると、コントローラチップＡ３６２０で制御されるインターフェースモードに移行するようにする。なお、図３６においては、フラッシュメモリチップ１３０がコントローラＡ３６２０と接続されているが、メモリチップ１３０が必要のないインタフェースがコントローラＡ３６２０で制御される場合、メモリチップ１３０はコントローラＡ３６２０と接続されなくてもよい。また、図３６において、メモリチップ１３０はコントローラＢ３６３０と接続されていないが、コントローラＡ３６２０を経由して、或いは直接接続されていてもよい。更に、図３６では、コントローラＡ３６２０並びにコントローラＢ３６３０が物理的に存在する場合について記載しているが、一つのコントローラで多種類のインタフェース制御を行い（エミュレーション）、上述のモードの切り替えによってインターフェースモードを切り替えることも可能である。また、異なるインタフェースを切り替えるだけでなく、同一のインタフェースにおいてバージョンごとにインタフェースを切り替えることも可能である。

【０１１７】本発明の実施形態によれば、メモリカード外部からＩＣチップの駆動クロックを直接供給しないため、ＩＣチップの処理時間を正確に計測できず、また、処理の実行タイミングや順序の検出が困難になる。さらに、異常な駆動クロックを供給することができず、演算エラーを発生させるのが困難になる。したがって、タイミング解析、電力差分解析、故障利用解析攻撃法に対するセキュリティが向上する。

【０１１８】本発明の実施形態によれば、メモリカード外部からＩＣチップの制御方式を自由に設定できる。例えば、高速処理が要求されるならば、ＩＣチップの駆動クロックの周波数を高くした制御方式を設定し、低消費電力が要求されるならば、ＩＣチップの駆動クロックの周波数を低くしたり、ＩＣチップの駆動クロックを適度に停止させる制御方式を設定することができる。したがって、セキュリティシステムの要求する処理性能に柔軟に対応したセキュリティ処理が実現できる。

【０１１９】本発明によれば、ＩＣチップによるセキュリティ処理に必要なデータや、ＩＣチップを管理するための情報を、フラッシュメモリに保持することができる。したがって、セキュリティ処理の利便性を向上させることができる。

【０１２０】本発明の実施形態によれば、ＭＭＣの製造者や管理者が、ＭＭＣ内部のＩＣチップに直接アクセスすることができる。したがって、ＭＭＣ内部のＩＣチップの初期化やメンテナンスを、従来のＩＣカードと同様な方法で実現できる。

【０１２１】本発明の実施形態によれば、フラッシュメモリチップを備えたＭＭＣに、セキュリティ機能を追加する場合、セキュリティ評価機関の認証を予め受けたＩＣカードチップ追加搭載することによって、セキュリティ評価機関によるＭＭＣの認証が不要となるため、ＭＭＣの開発期間又は製造期間が短縮する。

【０１２２】本発明の実施形態によれば、１つのカード型記憶装置において、多種類のインタフェースをサポートし、その判別を適切に行うことにより、場合に応じて各々のインタフェースを使い分けることができ、利便性を向上することができる。

【０１２３】

【発明の効果】本発明によれば、記憶装置のセキュリティを向上するという効果を奏する。

【０１２４】更に、本発明によれば、記憶装置の使い勝手を向上するという効果を奏する。

【図面の簡単な説明】

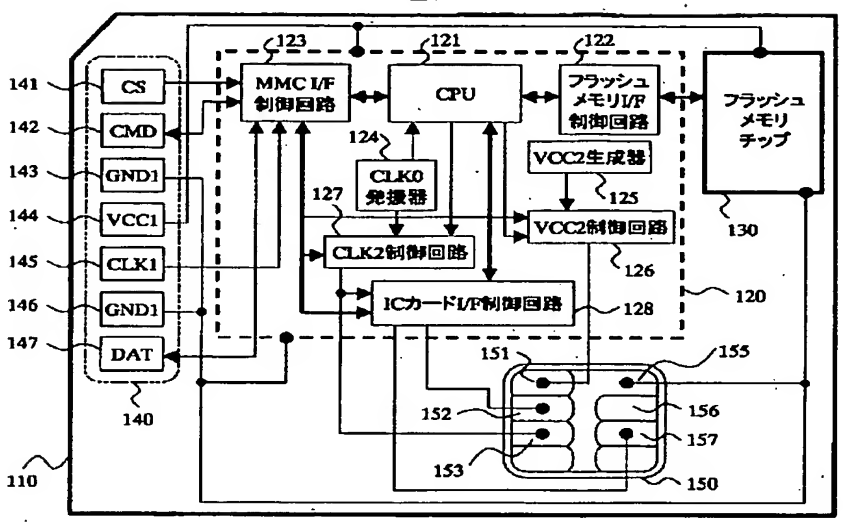
【図１】本発明を適用したＭＭＣの内部構成を示す図である。
【図２】本発明を適用したＭＭＣのホスト機器の内部構成、およびホスト機器とＭＭＣとの接続状態を示す図である。
【図３】ＩＣカードチップのコールドリセット時の信号波形を示す図である。
【図４】ＩＣカードチップのウォームリセット時の信号波形を示す図である。
【図５】ＩＣカードチップのＩＣカードコマンド処理時の信号波形を示す図である。
【図６】ＩＣカードチップの非活性化時の信号波形を示す図である。
【図７】ホスト機器によるＭＭＣへのアクセスを示したフローチャートである。
【図８】ＩＣカード制御パラメータとそれに対応するＩＣカードへの処理内容を示す表である。
【図９】ＩＣカードチップに対する第１次ＩＣカード初期化の詳細なフローチャートである。
【図１０】ＩＣカードチップに対する第２次ＩＣカード初期化の詳細なフローチャートである。
【図１１】非活性状態のＩＣカードチップに対するＩＣカード初期化時の信号波形を示す図である。
【図１２】活性状態のＩＣカードチップに対するＩＣカード初期化時の信号波形を示す図である。
【図１３】ＩＣカードチップによるセキュリティ処理の詳細なフローチャートである。
【図１４】セキュリティ処理要求ライトコマンドを処理するときの信号波形とフラッシュメモリチップアクセスを示す図である。
【図１５】ＩＣカードチップによるセキュリティ処理実行時の信号波形とフラッシュメモリチップアクセスの一例を示す図である。
【図１６】セキュリティ処理結果リードコマンドを処理するときの信号波形とフラッシュメモリチップアクセスを示す図である。
【図１７】インタフェース直通モードにおけるＭＭＣ外部端子とＩＣカードチップ外部端子の対応関係を示す図である。
【図１８】インタフェース直通モードへ移行する処理とインタフェース直通モードから復帰する処理のフローチャートである。
【図１９】インタフェース直通モードへ移行する処理時の信号波形を示す図である。
【図２０】インタフェース直通モードから復帰する処理時の信号波形を示す図である。
【図２１】フラッシュメモリチップの内部構成を示す図である。
【図２２】本発明を適用したＭＭＣの内部構成を簡単に示す図である。
【図２３】本発明を適用したＭＭＣをコンテンツ配信に応用した例を示す図である。
【図２４】本発明を適用したＳＤカードの内部構成を簡単に示す図である。
【図２５】本発明を適用したメモリースティックの内部構成を簡単に示す図である。
【図２６】本発明のＩＣカードチップの内部構成を示す図である。
【図２７】本発明を適用したカード型記憶装置の内部構成を示す図である。
【図２８】モード選択回路２７１０を中心とした入出力バスの接続状態を示す図である。
【図２９】本発明を適用したホスト機器におけるＩＣカード制御に関連するモジュール構成を示す図である。
【図３０】本発明を適用したカード型記憶装置及びＭＭＣソケットの一構成例を示す図である。
【図３１】記憶装置挿入時の手順を示すフローチャートである。
【図３２】本発明を適用したカード型記憶装置の概観を示す図である。
【図３３】本発明を適用した他のカード型記憶装置の概観を示す図である。
【図３４】本発明を適用したＭＭＣソケットの一例を示す図である。
【図３５】本発明を適用したスイッチの装備例を示す図である。
【図３６】本発明を適用した他のカード型記憶装置の内部構成を示す図である。

【符号の説明】

１１０…ＭＭＣ、１２０…コントローラチップ、１４０…ＭＭＣ外部端子、１５０…ＩＣカードチップ、１５１…ＶＣＣ２端子、１５２…ＲＳＴ端子、１５３…ＣＬＫ２端子、１５５…ＧＮＤ２端子、１５６…ＶＰＰ端子、１５７…Ｉ／Ｏ端子、２２０…ホスト機器、１４０５…ライトコマンド発行、１９０６…モード移行時刻、２００３…モード復帰時刻、２７０１…カード型記憶装置、２７１０…モード選択回路、２７２０…モード選択信号、２９１０…ＭＭＣソケット、２９３０…モード検出回路、２９４０…モード検出信号、３０１０…スイッチ、３６２０…コントローラチップＡ、３６３０…コントローラチップＢ。

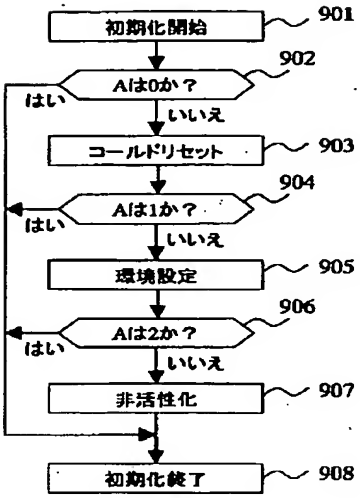
【図１】

図1



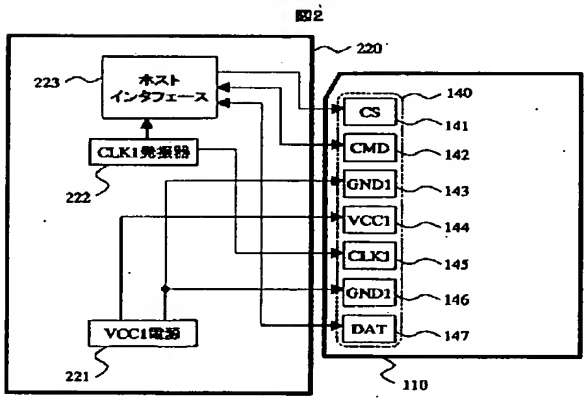
【図９】

図9



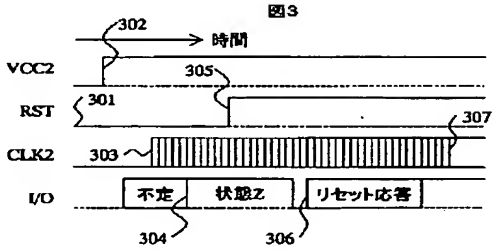
【図２】

図2



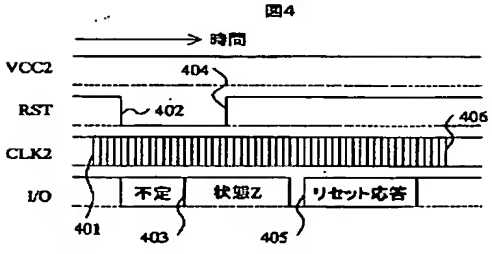
【図３】

図3



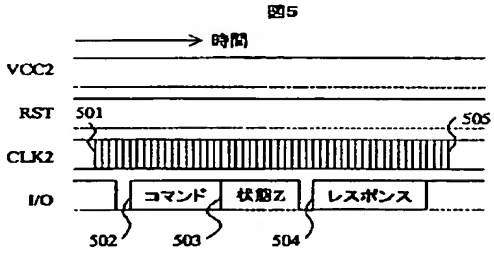
【図４】

図4



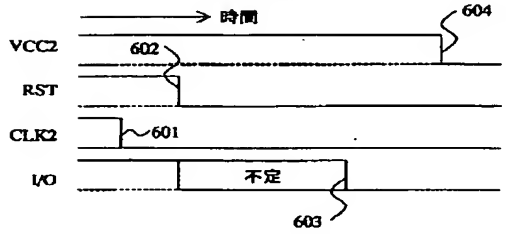
【図５】

図5



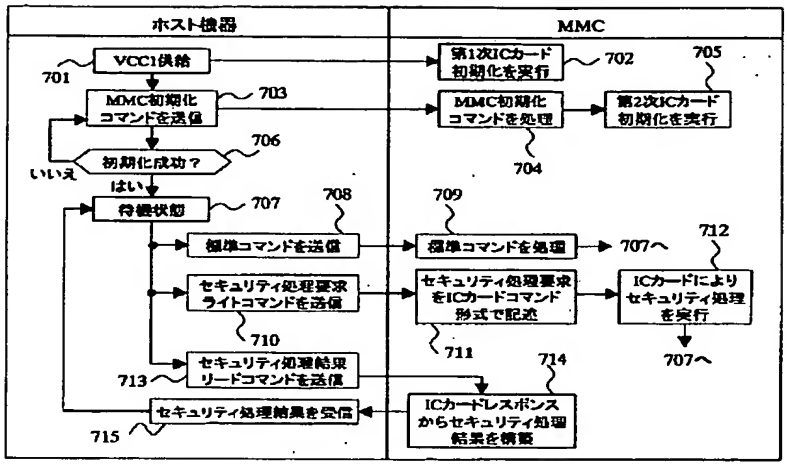
【図６】

図6



【図７】

図7



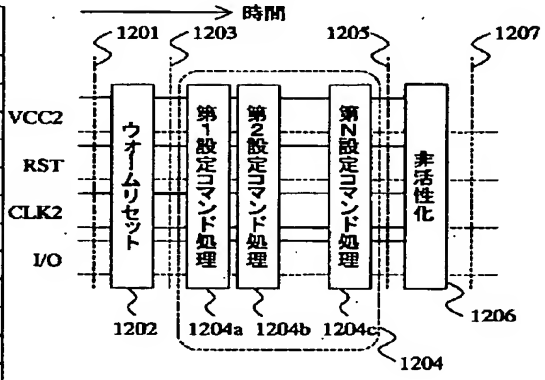
【図８】

図8

ICカード制御パラメータ		ICカードに対する処理
A=0		MMCのパワーオン時に，何もしない
A=1		MMCのパワーオン時に，リセット
A=2		MMCのパワーオン時に，リセットと環境設定
A=3		MMCのパワーオン時に，リセットと環境設定し，非活性化
B=0		MMCの初期化時に，何もしない
B=1	C=1	MMCの初期化時に，リセット
	C=2	MMCの初期化時に，リセットと環境設定
	C=3	MMCの初期化時に，リセットと環境設定し，非活性化
B=2	C=2	MMCの初期化時に，環境設定
	C=3	MMCの初期化時に，環境設定し，非活性化
B=3		MMCの初期化時に，活性状態ならば，非活性化
D=0		セキュリティ処理後に，非活性化しない
D=1		セキュリティ処理後に，非活性化する

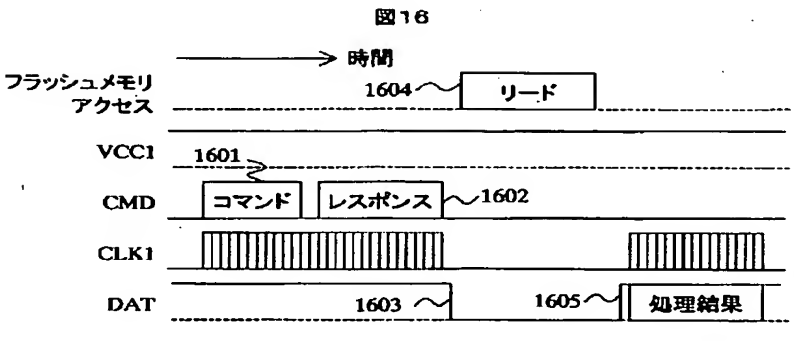
【図１２】

図12



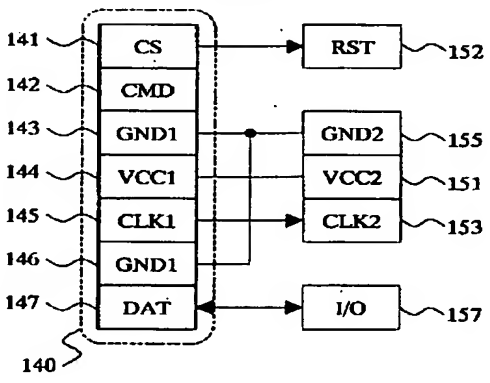
【図１６】

図16

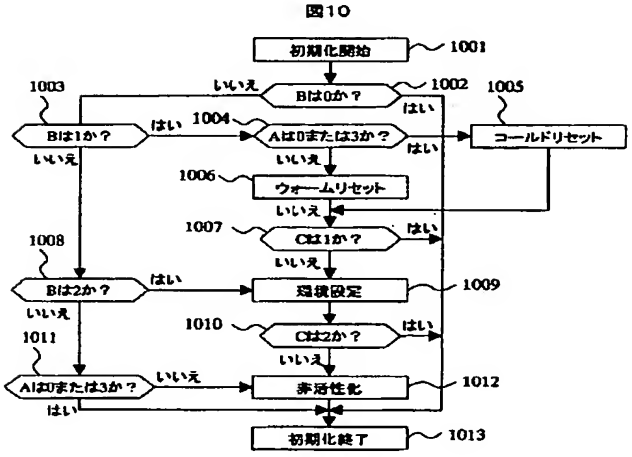


【図１７】

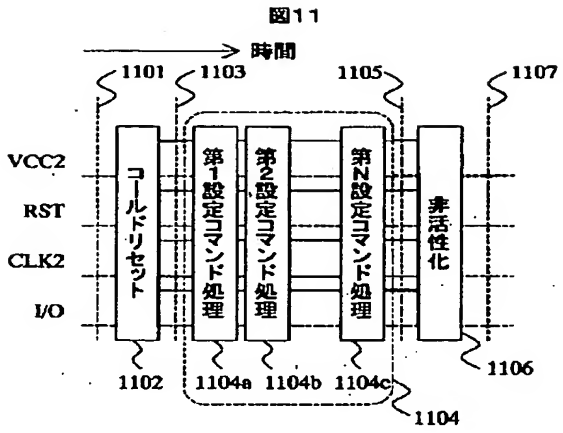
図17



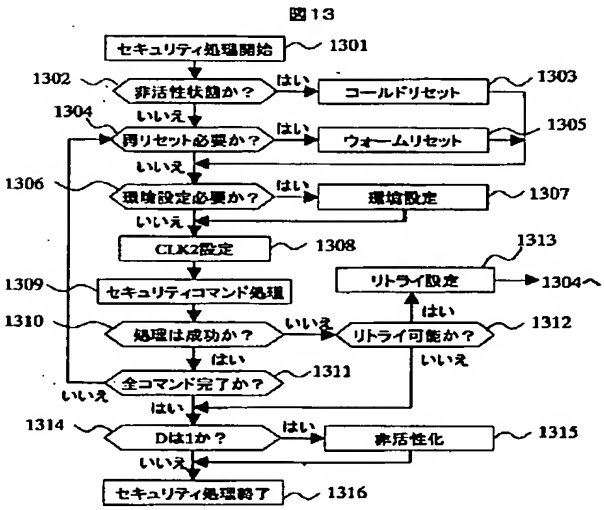
【図１０】



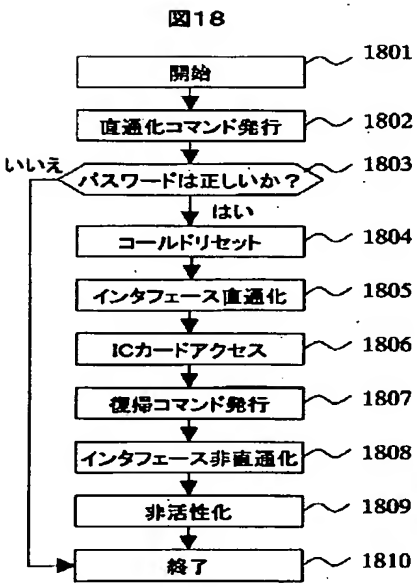
【図１１】



【図１３】

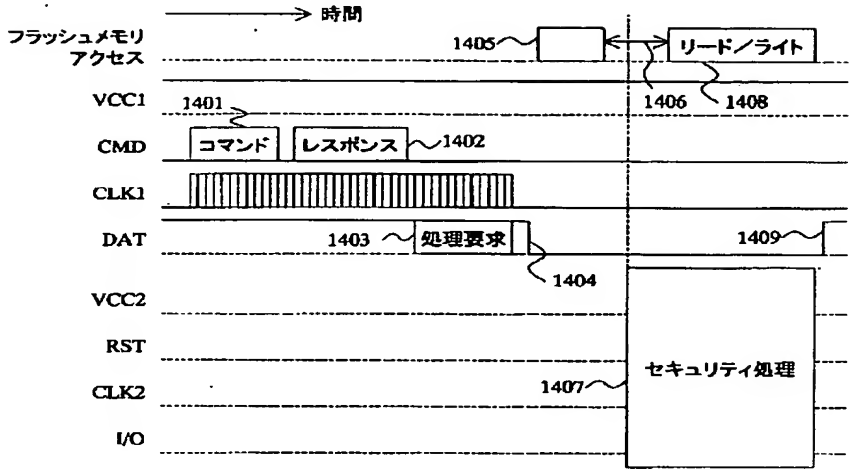


【図１８】



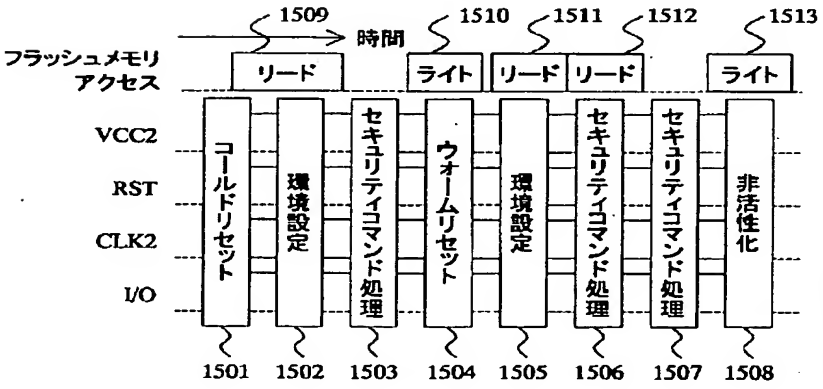
【図１４】

図14



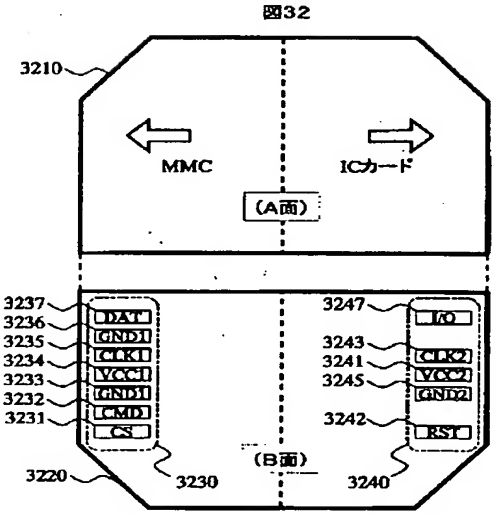
【図１５】

図15



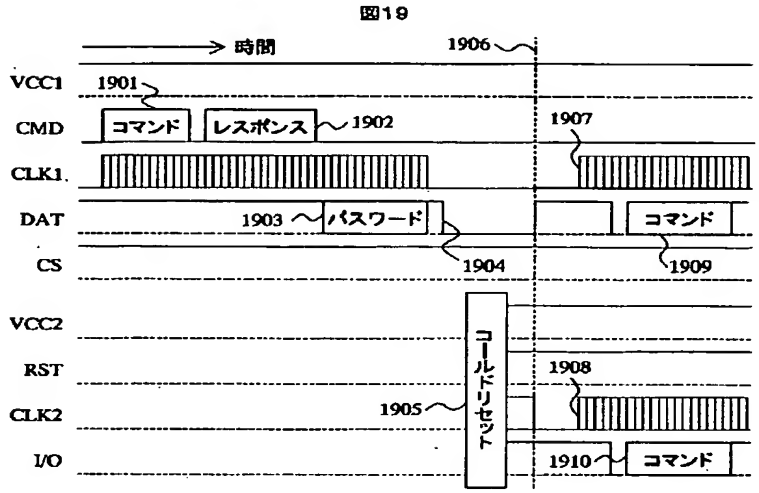
【図３２】

図32



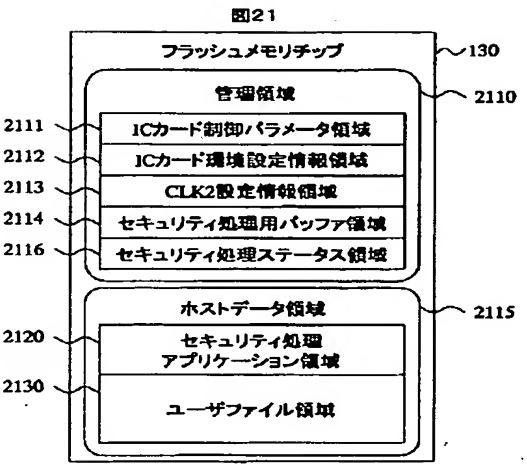
【図１９】

図19



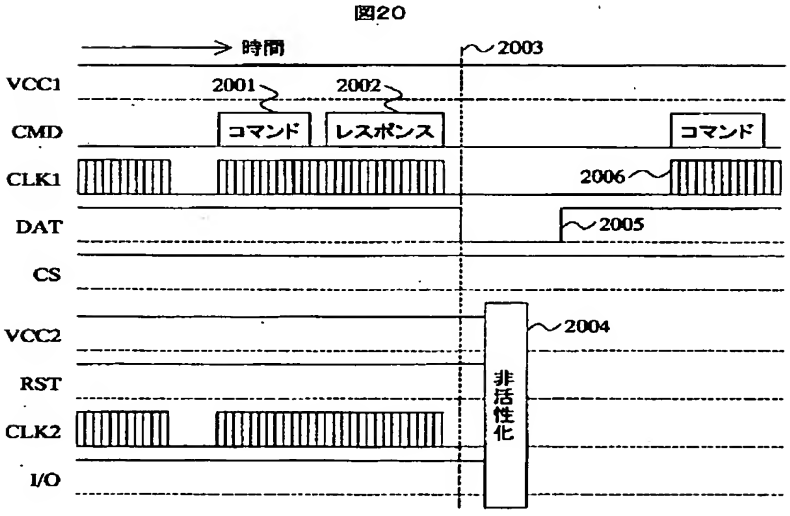
【図２１】

図21



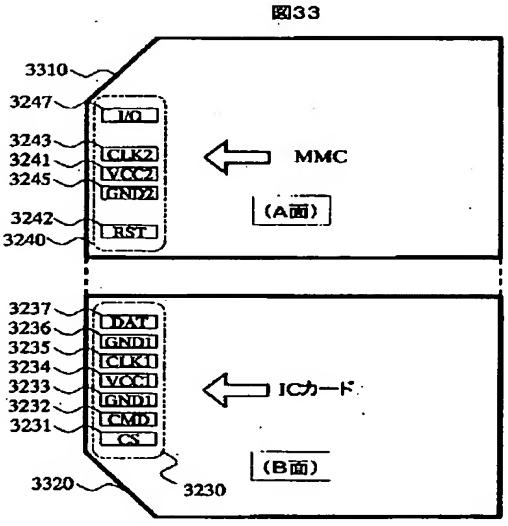
【図２０】

図20



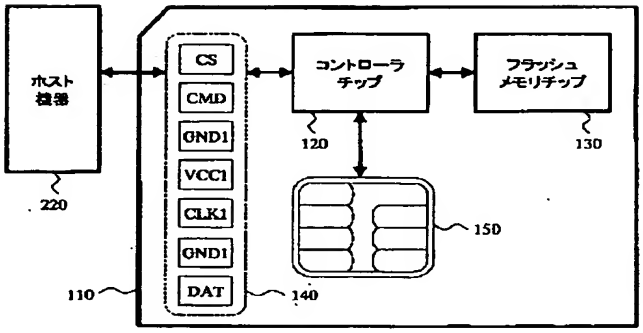
【図３３】

図33



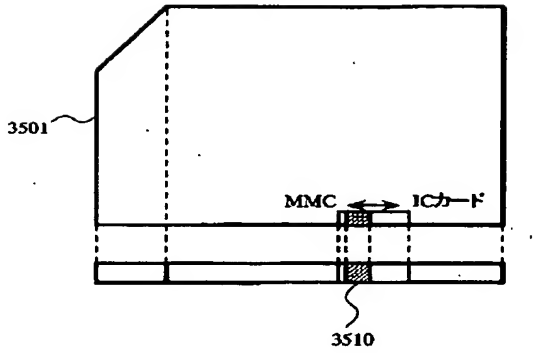
【図２２】

図22



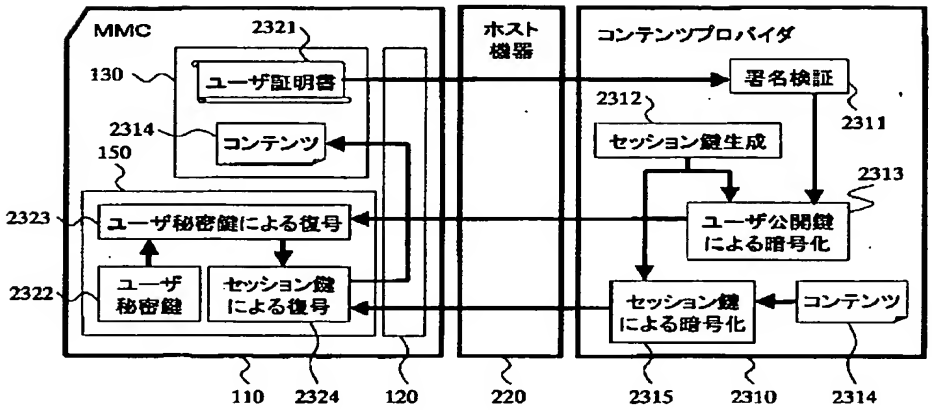
【図３５】

図35



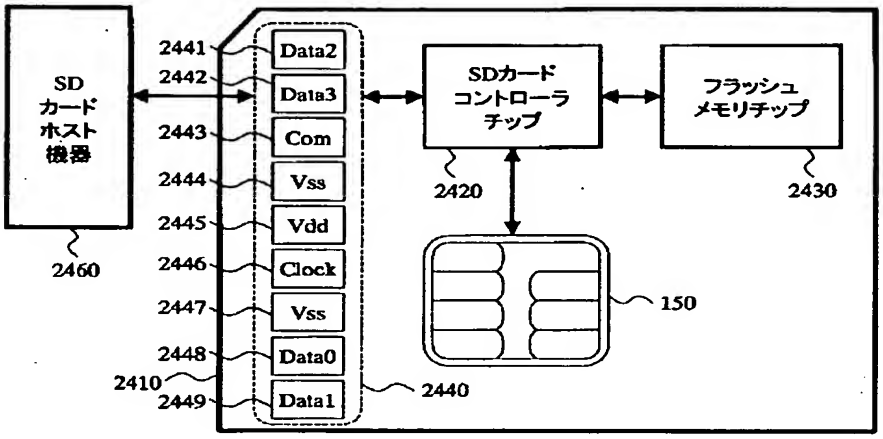
【図２３】

図23



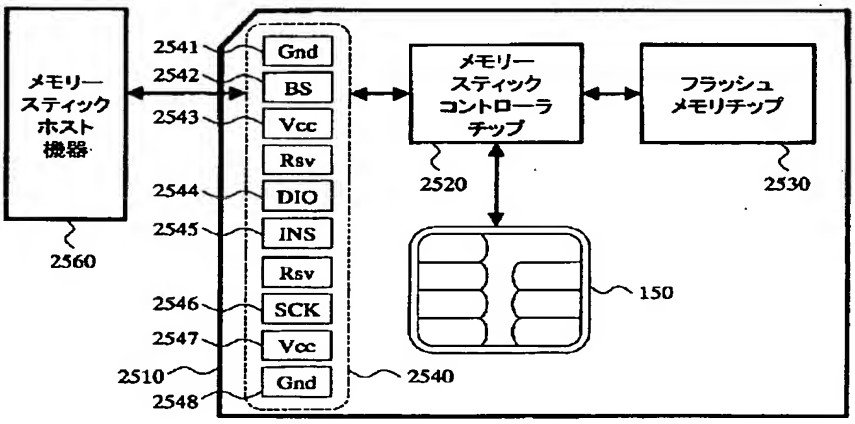
【図２４】

図24



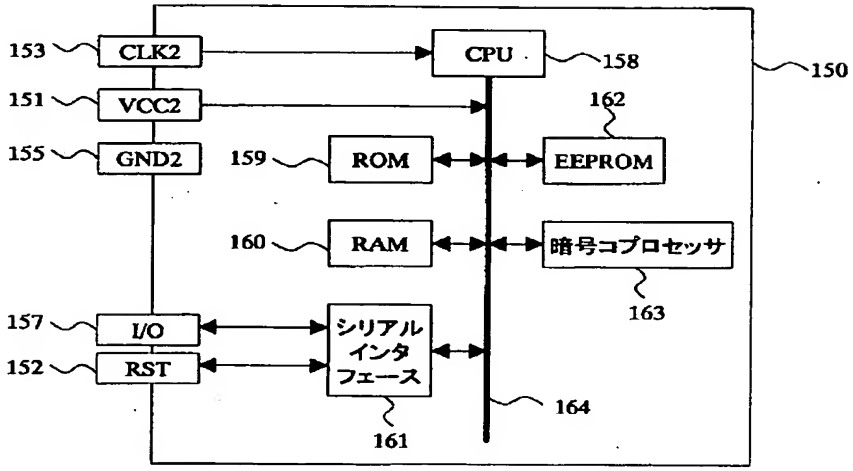
【図２５】

図25



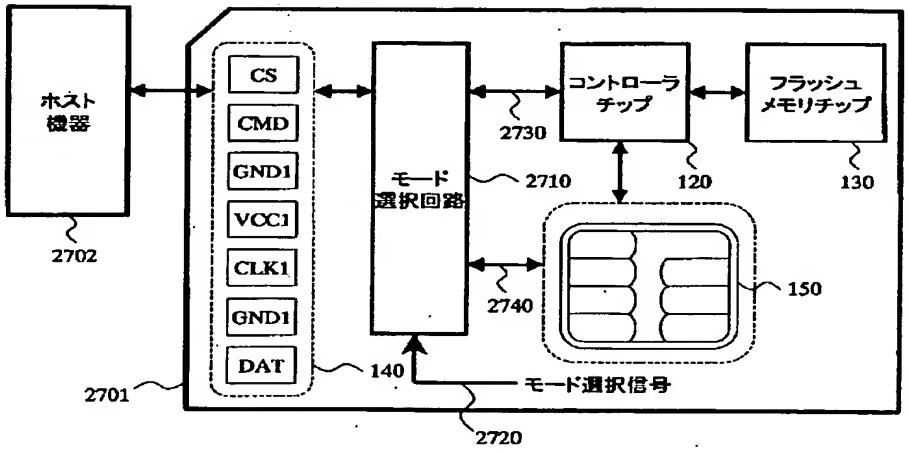
【図２６】

図26



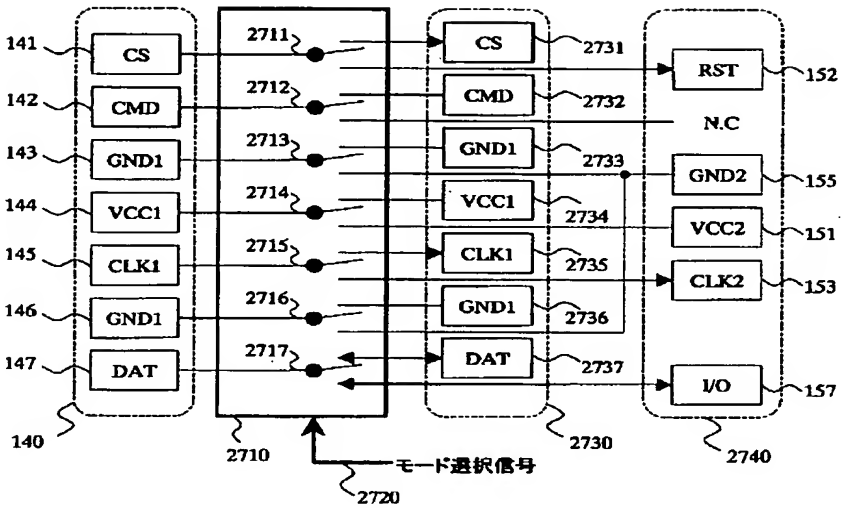
【図２７】

図27



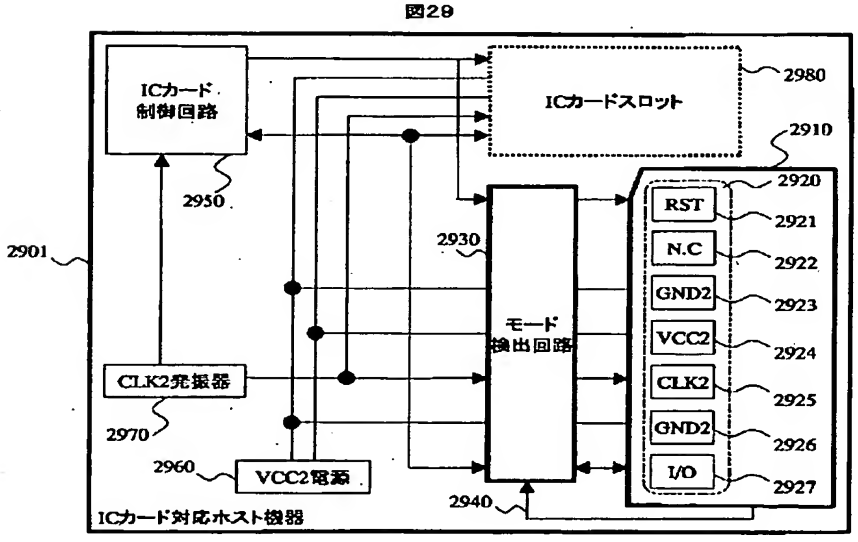
【図２８】

図28



【図２９】

図29



【図３０】

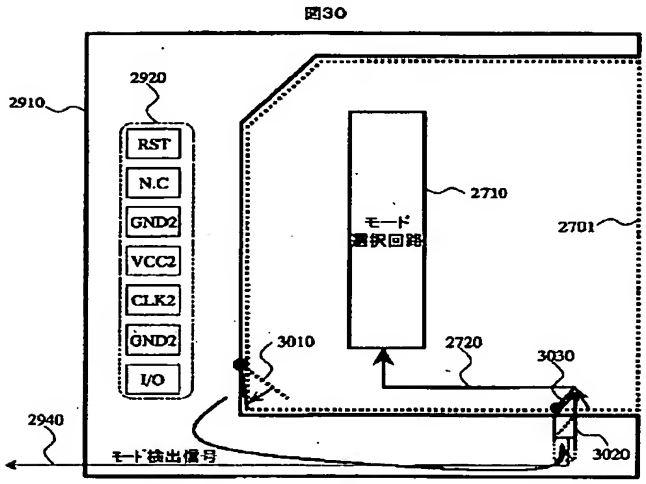


図30
2910
2920
RST
N.C
GND2
VCC2
CLK2
GND2
I/O
2710
モード
選択回路
2701
3010
2720
3030
2940
モード抽出信号
3020

【図３１】

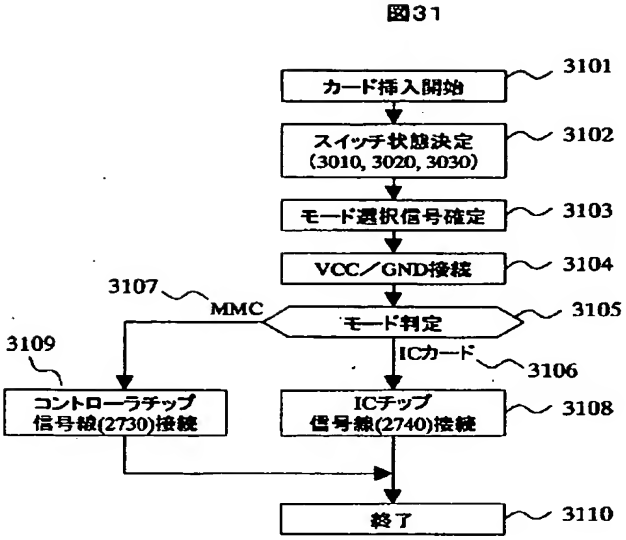


図31
カード挿入開始
3101
スイッチ状態決定
(3010, 3020, 3030)
3102
モード選択信号確定
3103
VCC／GND接続
3104
3107
MMC
モード判定
3105
3109
ICカード
3106
コントローラチップ
信号線(2730)接続
ICチップ
信号線(2740)接続
3108
終了
3110

【図３４】

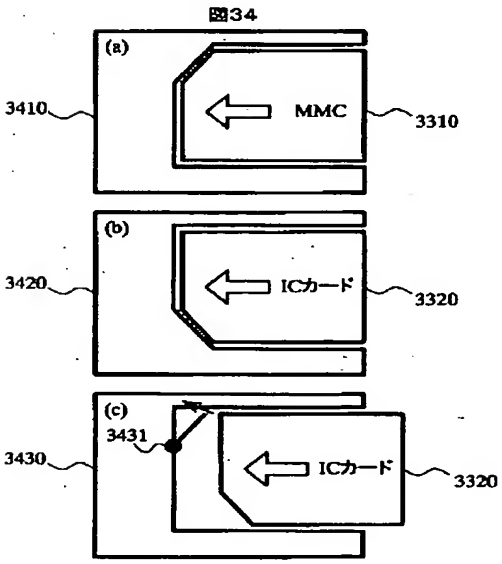
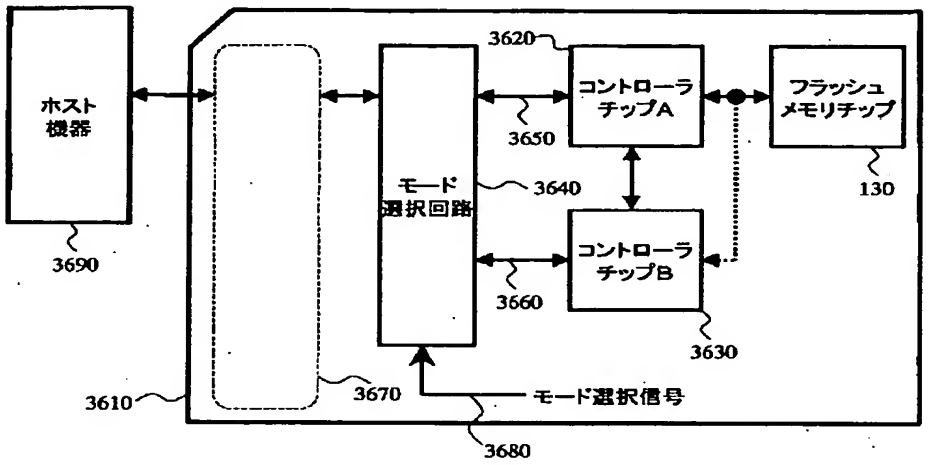


図34
(a)
3410
MMC
3310
(b)
3420
ICカード
3320
(c)
3431
3430
ICカード
3320

【図３６】

図36



フロントページの続き

(72)発明者　片山　国弘
東京都小平市上水本町五丁目20番１号　株式会社日立製作所半導体グループ内

25　Ｆターム(参考)　5B025 AE00 AE10
5B035 AA11 AA13 BB09 CA07 CA11 CA22
5B058 CA13 CA23 CA26 CA27 KA02 KA04 KA21 KA31 YA20